FINAL

JOINT INTEROPERABILITY AND ENGINEERING ORGANIZATION

System Administration Manual

rev 0

29 September 1995

GCCS-SAM-2.1

SYSTEM ADMINISTRATION MANUAL
GCCS VERSION 2.1

SUBMITTED BY:
James M. Quetsch
Major, USAF
Integration/Implementation
Branch Chief

APPROVED BY:
Ellis K. Conoley
Colonel, USAF
Program Manager, GCCS

TABLE OF CONTENTS

Section Page

Section Page

Section Page

Section Page

Section Page

Section Page

Section Page

Section Page

List of Tables

Table Page

List of Figures

SECTION 1. SCOPE

The Global Command and Control System (GCCS) is an Automated Information System (AIS) supporting the Department of Defense (DoD). GCCS is producing, integrating, and fielding new hardware and software components designed to provide the Joint Planning and Execution Community (JPEC) with new technology and functionality. GCCS system integration emphasizes use of commercial off-the-shelf (COTS) products, and merges the capabilities of a modern Local Area Network (LAN), UNIX-based client/server architecture, desktop-style Graphical User Interface (GUI), and a Relational Database Management System (RDBMS).

GCCS is intended to help Joint operation planners satisfy their deliberate and crisis planning responsibilities via access to a useful, user-tested, integrated set of analytic tools and flexible data transfer capabilities. The GCCS client/server architecture provides a firm foundation for linking external systems and GCCS components, permitting easy access to applications, and faster, more reliable, data transfers within a secure environment. At the heart of GCCS is a large database and application server connected to a LAN. The GCCS LAN interconnects the GCCS server with a variety of workstations (DOS and Microsoft Windows PCs, Macintosh, UNIX, and other X-Windows clients) that run associated software and application packages. The GCCS LAN will also connect with Wide Area Networks (WANs) supporting standard LAN design.

The GCCS architecture is specifically designed with flexibility and COTS standardization to allow interconnection with new networks and systems as they are deployed. This architecture will easily adapt to and assimilate new applications and functions.

GCCS is designed with the user in mind; powerful and flexible, yet fully functional. However, achieving these goals involves a complex system design, with a regular and effective technical, "behind the scenes" system administration (SA) activity. Consequently, trained SA personnel are absolutely essential to the satisfactory operation of the GCCS system resources at each site. This SA Manual provides technical system administration guidance for DoD sites receiving GCCS Version 2.1

1.1 Overview of this Manual

This manual:

- Provides guidance to sites on establishing SA positions, prerequisites, and qualifications.

- Describes the responsibilities of the GCCS SA with reference to specific Sun Microsystems Corporation products. (SunOS 5.3 designates the operating system only. Solaris 2.3 designates the distributed computer environment software.)

- Provides guidance to GCCS SAs on executing their responsibilities.

- Provides instructions to GCCS SAs on where to get further assistance.

This manual will not restate:

- Standard platform-specific (i.e., SunOS, HP-UX) documentation (each GCCS site will receive separately); or

- GCCS system and applications user documentation,

BUT will address user-specific database issues.

SECTION 2. LIST OF DOCUMENTS

2.1 Mail Administration Documents

sendmail, by Bryan Costales with Eric Allman & Neil Rickert,
published by O'Reily & Associates.

sendmail - An Internetwork Mail Router, by Eric Allman (SMM-16)

sendmail - Installation and Operation Guide, by Eric Allman (SMM-07)

Also useful are these Requests for Comments (RFC's):

RFC822	*Standard for the Format of ARPA-Internet Text Messages*
RFC821	*Simple Mail Transfer Protocol*
RFC819	*The Domain naming Convention for Internet User Applications*
RFC1123	*Requirements for Internet hosts - Application and Support*.

2.2 Domain Name Service (DNS) Administration Documents

Administrating NIS+ and DNS (Solaris Manual)

DNS and BIND (O'Reilly & Associates, Inc, Paul Albiztz & Cricket Liu)

2.3 Other Documents

Airfields Software Users Manual, 28 February 1995.

Airfields Software Center Operator Manual, 31 March 1995.

ESI JOPES External System Interfaces (ESI) Maintenance Manual, 15 May 1995.

FRAS (Fuel Resource Analysis System) Operators Manual, 23 June 1995.

GCCS Security Policy, 23 December 1993.

GCCS Automated Information System (AIS), Security Plan, 1 May 1995.

GCCS 2.1 Software Users Manual, 16 June 1995.

GCCS Ad Hoc Query User Manual, 14 April 1995.

GRIS CSCI v2.2 Operations Manual, 30 May 1995.

GSORTS User's Guide, 19 August 1994.

HP NetMtris Power Agent Users Guide (Volume 1, 2 and 3) Version 4.5, 25 May 1995.

JMCIS 2.1 System Administrators Guide, 15 July l994.

JMCIS 2.1 Security Managers Guide, 15 July 1994.

JOPES Administration Manual, 26 August 1991.

MEPES (Medical Planning and Execution System) Core Users Manual (UM), 1 November 1994.

MEPES (Medical Planning and Execution System) Core Technical Manual (UM), 1 November 1994.

NUCWA Users Manual (UM), 1 January 1993 (SECRET).

PREDEFINED Reports Users Manual, 31 May 1995.

UCCS Automated Message Handling Segment (AMHS) System Administrator/Operator Guide, 15 September 1993.

RDA (Requirements Development and Analysis) Build 2 Users Manual, 7 June 1995.

TARGET Users Manual, 30 December 1994.

SECTION 3. SEGMENT INSTALLATION

3.1 Overview

In GCCS, all software is packaged in modules called software segments. An application may comprise one or more segments, depending upon its complexity and modularity. The segments are provided to the site on 4mm or 8mm tapes, via ftp over the SIPRNET, or can be installed remotely by a repository site (Operational Support Facility or CINC) using the Remote Installer. The segments are installed using the Segment Installer tool, which comes with the GCCS COE Kernel. It is available when the SA logs in as **sysadmin**.

3.2 Setting Up Network Segment Installation Servers

Network Segment Installation servers are GCCS platforms on which software segments can be loaded and stored. The Segment Installer can then use the Segment Installation servers to install applications on other platforms. This eliminates the need for using tapes to install segments and allows the SA to build several platforms simultaneously.

The Executive Manager server stores the Table of Contents for the Segment Installation servers in the directory */h/data/global/SysAdm/toc_load*, which is mounted by all systems. The table of contents, toc, identifies the segments available on the network, and the platforms storing each segment. The actual segments are stored in the */home2* directory on the Segment Installation server. The SA should insure that */home2* has sufficient space to accommodate the required segments; if space is limited, the SA can set up separate platforms as Network Installation servers. The following are the steps for setting up a Segment Installation server:

a. If, during the installation of the GCCS COE Kernel tape, the question:

   "Is this going to be a Segment Installation Server? (y/n)[n]"

   was answered "y" then go to Step c.

   If the question was answered "n," and the site now wants to set the server up as a Segment Installation server, then go to Step b. before performing Step c.

b. Add the following line in */etc/dfs/dfstab*:

```
Share -F nfs -o anon=o /home2
```

   and execute the following command:

```
/etc/share /home2
```

c. Log in as **sysadmin** and select **INSTALLATION SERVER** from the SOFTWARE menu.

d. If the tape drive from which you will be loading the software segments is locally attached, and is device 0, go to Step e. Otherwise, click the **SELECT MEDIA** button.

   1. If the tape drive is on another platform, select **HOST** under HOST and then click on the field next to NAME. Enter the name or the IP address of the remote platform. Select **OTHER** under DEVICE and then click on the field under OTHER. Enter the correct drive number, ensuring that the "b" option is used (e.g., **`/dev/rmt/0mbn`**).

   2. If the tape drive is locally attached, select **OTHER** under DEVICE and then click on the field under OTHER. Enter the correct drive number, ensuring that the "b" option is used (e.g., **`/dev/rmt/1mbn`**).

e. Load the desired segment tape in the tape drive and select **READ TOC**.

f. Use the cursor to highlight the segments to be loaded. Highlight as many as desired.

g. Select **LOAD** to begin loading the selected segments. The segments will be installed in */home2* in the *NET_SERVER* directory. The Table of Contents will be stored in directory */h/data/global/SysAdm/toc_load*.

h. The Installation server will not load any segments after */home2* has reached 80 percent of its capacity. To override this constraint, position the cursor in the Segment Installer GUI, and press the right mouse button. Select **Disk Space Override** from the menu. A new window labeled "OVERRIDE DISK SPACE LIMITATIONS" will appear. Select the desired override (**90 percent** or **95 percent**) from this window and then **EXIT**. Continue loading segments after this.

i. To allow another platform to use the Segment Installation server, an *.rhosts* file must be created in the / directory. This file must have the host names of each platform in which the Segment Installation server will be used.

3.3 Using the Segment Installer

The segments are installed using the Segment Installer tool, which is a GUI that provides the following:

- Identification of which applications (segments) are loaded on your system.

- Identification of which applications (segments) are available on a tape or on a Segment Installation server.

- The capability to install and/or de-install applications (segments) on the system.

The Segment Installer installs software in the */h* file system. When this file system is approximately 80 percent full, the Segment Installer will install software in */home1*, followed by */home2*, */home3*, ..., */home99*. The 80 percent constraint can be overriden by using the **Disk Space Override** feature of the Segment Installer.

The Segment Installer tool can be invoked directly by logging in as **sysadmin** and launching it via the icon or menu pick, or by the Remote Installer tool (RemoteInst), addressed in Section 3.4. To use the Segment Installer do the following:

a. Log in as **sysadmin**.

b. Position the cursor over the **SOFTWARE** menu pick and select **Segment Installer**, or position the cursor over the **Install** icon in the Launch Window and double-click. The Segment Installer GUI will appear after approximately 15 seconds.

c. If loading from tape, and if the tape drive from which you will be loading the software segments is locally attached, and is device 0, go to Step e; otherwise click the **SELECT MEDIA** button. A "Checking Media" window will appear for approximately 30 seconds, sometimes longer. A window labeled "Select Media" will then appear.

d. In the "Select Media" window execute one of the following:

   1. If you are going to use the Segment Installation server, select **NETWORK** under DEVICE and then select **OK**.

   2. If the tape drive is on another platform, select **HOST** under HOST and then click on the field next to NAME. Enter the name or the IP address of the remote platform. Select **OTHER** under DEVICE and then click on the field under OTHER. Enter the correct drive number, ensuring that the "b" option is used (e.g., **`/dev/rmt/0mbn`**).

   3. If the tape drive is locally attached, select **OTHER** under DEVICE and then click on the field under OTHER. Enter the correct drive number, ensuring that the "b" option is used (e.g., **`/dev/rmt/0mbn`**).

e. Load the segment tape in the tape drive and select **READ TOC**. If using the Segment Installation server, simply select **READ TOC**.

f. The Segment Installer GUI will disappear, and a window containing an hourglass labeled "Checking Media" will be displayed. The "Checking Media" window will disappear and another hourglass window labeled "Busy" will be displayed, with a message "Reading Table of Contents."

g. The Segment Installer GUI will reappear with a list of available segments displayed in the window labeled "Table of Contents." Segments already installed will have an asterisk. (The Table of Contents and the *SegDescrip* directory for each segment listed are stored in */h/data/local/SysAdm/toc_load*, if loaded from tape, or in */h/data/global/SysAdm/toc_load* if network installed).

h. To select a segment for installation, move the cursor to the segment to be installed and click once. The segment will be highlighted.

NOTE: It is possible to select more than one segment for installation at a time, but it is not recommended, especially for segments larger than 20 MB. Never install more than one application database segment at a time.

i. To begin the install process, select the **Install** button. A window with an hourglass labeled "Installing Selected Segments" will appear in place of the Segment Installer GUI. The application and database segment tables located in Section 5 of the GCCS Implementation Procedures show approximately how long it takes to load each segment.

j. After the segment is installed, the Segment Installer GUI will reappear with another window overlaid signifying that the segment was either successfully or unsuccessfully installed.

k. If the segment was successfully installed, continue loading additional segments if required.

l. If the segment did not install successfully, a warning will appear stating that an "error occured while installing selected segment(s)." Click on **OK** to clear the warning and then select **STAT LOG** to determine why the segment(s) did not install.

The most common explanations for a segment not installing are:

- The required segments are not installed on the system.
- The segment is not JMCIS compatible.
- Insufficient disk space is available to install the segment.

To correct the "required segments not installed" problem, highlight the problem segment in the Table of Contents window, and select **REQUIRED**. Install any segments listed that are not currently installed. Also consult the Segment Dependency table in Section 5 of the *GCCS Implementation Procedures* for any additional dependencies. Pay particular attention to the version number of the required segments. If the version currently installed does not match the version specified for the required segments, the segment still may not install.

To correct the "not JMCIS compatible" problem, exit the Segment Installer and rewind the tape. After the tape is rewound, restart the Segment Installer and try again.

To correct the "insufficient disk space" problem, use the Disk Space Override feature of the Segment Installer (see Step n following).

m. If a segment did not install successfully, but is listed in the "SEGMENTS CURRENTLY INSTALLED" window of the Segment Installer, it should be de-installed before attempting to re-install it.

n. The Segment Installer will not load any segments after the available */h* and */home[1-99]* file systems have reach 80 percent of their capacity. To override this constraint, position the cursor in the Segment Installer GUI and press the right mouse button. Select **Disk Space Override** from the menu. A new window labeled "OVERRIDE DISK SPACE LIMITATIONS" will appear. Select the desired override (**90 percent** or **95 percent**) from this window and then **EXIT**. Continue loading segments after this.

3.4 Using the Remote Installer

The Remote Install (RemoteInst) function provides the following capabilities:

- It allows an operator at a remote site to "pull" software segment(s) from a repository site and load them in the remote site's Segment Installation server. The operator may also use RemoteInst to install the segment(s) on a platform after they are pulled.

- It allows an operator at a repository site the ability to download or "push" software segments to other sites where they are loaded into the site's Segment Installation server. It also provides the operator at the repository site the ability to install or de-install segments on platforms at other sites.

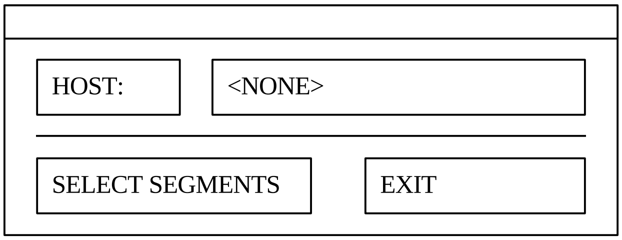
3.4.1 Using Remote Install for the Pull Operation. The Pull operation consists of an operator at the remote site grabbing and transferring software segments, made up of segment install file(s) and shell scripts, from the repository site to the remote site. The Pull operation has a graphical user interface intended for ease of use.

NOTE: Prior to executing the following steps, the Remote Install segment must be installed.

To run the Remote Install in Pull mode, do the following:

a. At the remote site, log onto a platform as **sysadmin**.

b. Select **Remote Install** from the "Software" menu or double-click on the **Remote Install** icon. This brings up a window like that shown in Figure 3-1.



HOST: <NONE>

Figure 3-1. Remote Install Window

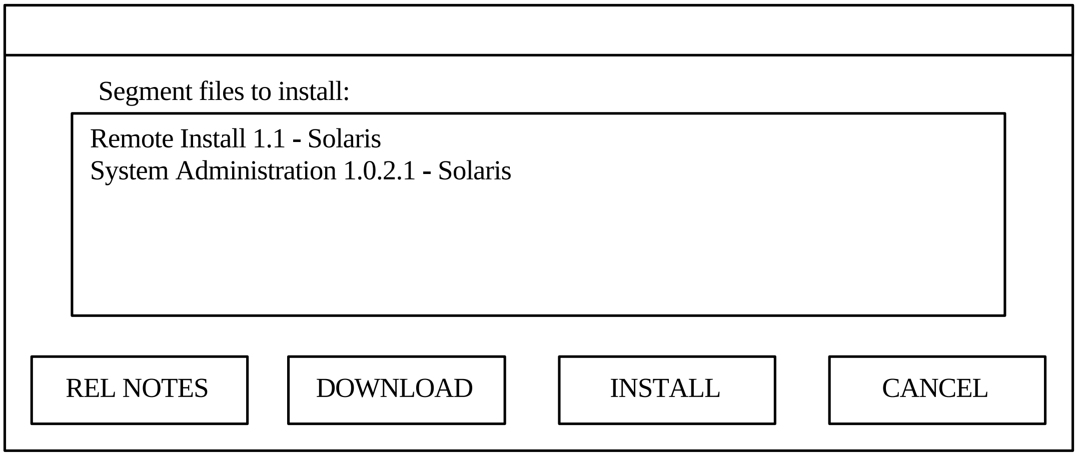
c. Enter the name of the repository host in the text field containing the word "<NONE>".

d. Select **SELECT SEGMENTS.** This will connect to the repository machine and bring up the screen shown in Figure 3-2, which contains a list of segments available for pulling from the repository site:

NOTE: If the repository site machine is not set up correctly, the following message will appear:

```
"No segments found on the specified host   "
```

Consult Section 3.4.3 for instructions on configuring a repository site.



Segment files to install:

Remote Install 1.1 - Solaris
System Administration 1.0.2.1 - Solaris

Figure 3-2. Select Segments Screen

e. Select the segment(s) to be pulled by moving the mouse to the desired segment and clicking once. The segment(s) will be highlighted.

f. To pull the segment and load it on the site's network Segment Installation server, select **DOWNLOAD**.

g. To install the segment on the platform executing Remote Install, in addition to loading it on the network Segment Installation server, select **INSTALL.**

h. Progress will be indicated by the following series of messages:

```
Transferring files
Formatting segments
Launching Installer (only if INSTALL was selected)
```

i. If **INSTALL** was selected, the Segment Installer will appear after the segments are transferred. Follow the procedures in Section 3.3 to use the Segment Installer.

3.4.2 Using Remote Install for the Push Operation. The Push operation consists of an operator at the repository site (Operational Support Facility or CINC) sending the Segment Install File and shell scripts from the repository site to the client (remote) site. The operator has the ability to load the segment on the remote site's Network Installation server (Segment Installation server) and install/de-install segments on the remote site's platforms. The Push operation uses only a command line interface, as follows:

RemoteInt [-p -l -i] <hostname> <segment install file>

Where:

-p indicates that the Remote Installer should only send the file across the network and load it on the Network Segment Installation server specified in <hostname> in the directory */home2/NET_SERVER*. It does not install the segment on the remote site.

-i indicates that the tool should send the file and install the file on the Network Segment Installation server specified in <hostname>, and then launch the Segment Installer on the remote machine so the Remote Install operator can go ahead and install the segment.

-l indicates that the tool should launch the remote machine's Segment Installer so that it is displayed on the repository machine's display.

<hostname> is the host name or IP address of the machine at the remote site on which the segment will be installed. For option **-p** + **-i** host name must be the name of a Network Segment Installation server.

<segment install file> is the full path of the segment install file that is to be installed. Only one segment install file may be installed at a time.

3.4.2.1 Remote Install Push Example.

The following is an example of a Push operation. In the example, a segment file named *RemoteInstall_1.1.tar*, located under */home10/ftp/pub/RemoteInstall* at the repository site, is installed on the remote site's Network Installation server machine, named *jdeftest.jdef*, without launching the installer on the remote machine:

a. **RemoteInst -p jdeftest.jdef /home10/ftp/pub/RemoteInst/RemoteInstall_1.1.tar**

b. The operator will then be prompted for valid user ID and password on the machine to which the segment is being pushed. Enter ***root*** or ***sysadmin*** as a valid user ID.

c. After entering the correct user ID and password, the operator would see a series of messages similar to the following:

```
Checking remote system type...
Attempting to get free space from remote machine...
Free Disk Space on Remote Machine == 255428 KB

Installing Segment File [/home10/ftp/pub/RemoteInst/RemoteInst_1.1.tar]
This can take a while - - please be patient.

Sending file:  RemoteInst_1.1.tar
100%   0   ========================>      2447360 bytes.  ETA:   0:00
2447360 bytes sent in 2.19 seconds,  1.06 MB/s.
Sending file:   AddToNetTOC
100%   0  ===========================>  7415 bytes.  ETA:  0:00
7415  bytes sent in 0.03 seconds,  276.14 kB/s

Formatting segment on remote machine...    [Network Installation Server]
```

```
Expanding the segment file (this may take a while)...     [Extracting the tar file]

Adding new segment to the table of contents...

Adding segment to the network installer...

Cleaning up ...  Please be patient

Network install completed
   *** Remote Install Completed ***
```

3.4.2.2 Remote Install Install/De-install Example.

To de-install and/or install segments on a remote machine, Remote Install provides the ability to launch the remote machine's Segment Installer on the repository machine's display. This uses a command line interface, as follows:

a. **RemoteInst -l 199.114.208.77**

b. The operator will then be prompted for valid user ID and password on the remote machine on which the Segment Installer is being launched.

c. The Remote Install tool will transfer a file to configure the account for using the Segment Installer. Finally, the installer will be launched on the remote display. During this process the operator will see the following messages:

```
Checking remote system type...
Attempting to get free space from remote machine...
User sysadmin logged in.
Sending file:   LaunchInstaller
100%  0   ============================  1396 bytes. ETA:     0:0
0
1396 bytes sent in 0.05 seconds,  24.98 kB/s.
Launching Segment Installer on 121.0.0.125:0.0
```

d. At this point, the Segment Installer will appear on the repository machine's display. Follow the procedures in Section 3.3 to use the Segment Installer to install/de-install segments on the remote machine.

3.4.3 Configuring a Repository Site for Pull Operation. For the Pull operation to work, the repository site needs to be configured properly. First, the Pull works by using anonymous ftp. Refer to the manual pages for "ftpd" for information on setting up anonymous ftp. Once anonymous ftp is configured, some additional files need to be added under the *ftp* home directory:

~ftp/pub/SegFiles

This file contains data on the segment install files. It is a plain text file that contains one line for each segment install file on the system. The line contains three fields that are separated by colons, as:

```
<description>:<relative segment file path>:<relative release notes path>
```

Where:

<description>: is the description that will appear on the Remote Install window when a user attaches to the repository site using the Pull operation (Section 3.4.1). The field should contain at a minimum the segment name, the version number, the machine type, and the file size.

<relative segment file path>: is the path and name of the segment install file [local tar file].

<relative release notes path>: is an optional field that indicates the path and file name of the release notes files.

A valid *SegFiles* file would look like the following:

```
Remote Install 1.1:/pub/RemoteInst/RemoteInst_1.1.tar: /pub/RelNotes/RemoteInst.RN
JMTK 1.0 for Solaris:/pub/JMTK/JMTK_1.0.tar:/pub/JMTK/JMTK_1.0.RN
System Administration 1.0.2.1:/pub/SysAdm/SysAdm.1.0.2.1.tar:
```

```
    ~ftp/pub/ShellScripts/AddToNetTOC
    ~ftp/pub/ShellScripts/LaunchInstaller
```

The two files in bold face above are distributed with the Remote Install segment. They are shell scripts that load the pulled segment(s) on the Network Installation server [*AddToNetTOC*] and launch the Segment Installer [*LaunchInstaller*]. They can be found under */h/RemoteInst/progs* after the Remote Installer segment has been installed.

NOTE: All segment install files must reside under the *~ftp/pub* directory for the Pull function of Remote Install to work.

SECTION 5. DOMAIN NAME SERVICE ADMINISTRATION

5.1 Overview

Every network device attached to a TCP/IP network is identified by a unique 32-bit IP address. Any device that has an IP address can be assigned a host name. While host names are not required--they simply make it easier for the user to use the network and may be used interchangeably with a system's IP address.

Currently three popular methods are used to translate or resolve host names into IP addresses in GCCS:

- Host Tables (/etc/hosts)
- NIS+
- Domain Name Service (DNS)

Host tables are located on each system on the network in the / *etc* directory. This requires that each table be maintained separately and, typically, can be an administrative burden on all but the smallest of networks.

When using NIS+, a single host file, found under *\/h/EM/nis_files/host* in the GCCS EM server, is used by all GCCS platforms. It should not be used to resolve names of platforms outside the site's LAN.

DNS is an application layer protocol that is part of the standard TCP/IP protocol suite. DNS is in essence a naming service; it obtains and provides information about hosts on a network.

DNS performs naming between hosts within the local administrative domain and across domain boundaries. It is distributed among a set of servers, commonly known as "name servers," each of which implements DNS by running a daemon called *named*.

5.2 References

1. *Administrating NIS+ and DNS* (Solaris Manual)

2. *DNS and BIND* (O'Reilly & Associates, Inc, Paul Albiztz & Cricket Liu)

3. DNS template files, which are loaded onto the designated DNS system in / *var*/*nameserver* by the GCCS COE Kernel tape, if the installer requests them. These files are also available from the Operational Support Facility (OSF) through an "anonymous ftp" account on the root domain name server "hornet" (IP address 199.114.100.20).

   Instructions for getting DNS Template files via ftp:

   ```
   host_name > ftp hornet<return>
   hornet login: anonymous<return>
   password: <no password is needed><return>
   ftp > cd pub/dns<return>
   ftp > mget *<return>
   ```

```
ftp > bye<return>
```

The installer will be prompted for the retrieval of each file in the DNS directory on *hornet*. Answer **yes** to those the site requires and **no** to those not required. These files will be placed in the directory the installer originally logged into at the beginning of the ftp session. It is best that the installer is in the /*var*/*nameserver* directory locally.

5.3 Pre-Installation Tasks

Before beginning the DNS installation, perform the following tasks:

a. Choose two reliable UNIX machines on the LAN to be the primary and secondary name servers. Any UNIX device with the *bind* or *in.named* daemon can run the name server software. These local name servers will be set up to know the addresses and aliases of all the local devices and to know where to look for information about devices in other domains. The name server software does not require dedicated machines.

NOTE: All *SIPRNET* domain names end with `gcc.smil`

b. Choose a DNS domain name. Table 5-1 provides a partial list. (Names listed can be verified by calling the Hotline at the DISA OSF.) A DNS domain name is not the same as the NIS or NIS+ domain name. The NIS or NIS+ domain name is what the user gets after entering the command *domainname*. Some examples of fully qualified DNS domain names are:

the osf uses:	`osf.gcc.smil`
the jdef uses:	`jdef.gcc.smil`
centcom uses:	`cent.gcc.smil`

c. Register site name servers with the root name server. To notify the OSF of a new name server, mail the fully qualified domain names of the name server hosts, their IP addresses, and a technical point of contact to " *net_adm@hornet.osf.gcc.smil*".

Table 5-1. Domain Names

GCCS DOMAIN E-MAIL ADDRESSES: <user-id>@<host-name>.<subdomain-name>.gcc.smil

GCCS SUBDOMAIN NAME/*alias*	**COMMAND**	**ADDRESS (CONTAINS S/A DESIGNATION)**
acc	ACC	Air Combat Command, Langley AFB, VA (AF)
acom/*usacom*	USACOM	US Atlantic Command, Norfolk, VA (Joint)
acom	MARFORLANT	Marine Forces Atlantic, Camp Lejeune, SC
acom	CINCLANTFLT	US CINC Atlantic Fleet, Norfolk, VA (NAVY)

Table 5-1. Domain Names (con't)

GCCS SUBDOMAIN NAME/*alias*	COMMAND	ADDRESS (CONTAINS S/A DESIGNATION)
afic	AFIC	Air Force Intelligence Command, Kelly AFB, TX
afmc	AFMC	Air Forces Material Command, Wright Patterson AFB, OH
afmpc	AFMPC	Air Force Military Personnel Center, Randolph AFB, TX
afres	AFRES	Air Force Reserves, Robins AFB, GA
afsoc	AFSOC	Air Force Special Operations Command, Hurlbert Field, FL
afspace	AFSPACE	Air Force Space Command, Peterson AFB, CO
afwc	AFWC	Air Force War College, AL
alcom	ALCOM	Alaskan Command, AK
amc	AMC	Air Mobility Command, Scott AFB, IL
anmcc	ANMCC	Alternate National Military Command Center (DISA)
aoc	AOC	Army Operations Center, Pentagon (Component HQDA)
areur	AREUR	Army, Europe, GE
arpac	ARPAC	Army, Pacific, Ft. Shafter, HI
arso-pan	ARSO	Army Southern Command, Ft. Clayton, Panama
arspace	ARSPACE	Army Space Command, Peterson AFB, CO
asoc	USASOC	US Army Special Operations Command, Ft. Bragg, NC
awc	AWC	Army War College, Carlisle, PA
cent	CENTCOM	US Central Command, MacDill AFB, FL
centaf	CENTAF	Air Force Central Command, Shaw AFB, SC
cno	CNO	Chief of Naval Operations, Pentagon
defor	COMICEDEFOR	Commander Icelandic Defense Forces, Iceland (ACOM)
foraz	COMUSFORAZ	Commander, US Forces, Azores, Lajes Field, Portugal (ACOM)
faisa	ARCENT	Army Central Command, Ft. McPherson AFB, GA
force1/*forscom*	FORSCOM	US Forces Command, Ft. McPherson (ARMY), GA
navcent	NAVCENT (FWD)	Navy Central Command (Forward), Bahrain
navcent	NAVCENT (FWD)	Navy Central Command (Forward), Saudi Arabia
hqaf	HQAF	HQ Air Force, Pentagon
hqda/*DAWN*	HQDA	HQ Department of the Army, Pentagon
hqeucom	EUCOM	European Command, GE (Army)
hqeucom	MARFOREUR	Marine Forces Europe, GE
hqmc	HQMC	HQ Marine Corps, Navy Annex, DC
jdef	JDEF	Joint Development & Evaluation Facility, VA Sq., VA (DISA)
jisc	JISC	DISA, Pentagon
jsoc	JSOC	Joint Special Operations Command, Ft. Bragg, NC

Table 5-1. Domain Names (con't)

GCCS SUBDOMAIN NAME/*alias*	COMMAND	ADDRESS (CONTAINS S/A DESIGNATION)
kttc	AETC	Air Education & Training Command, Keesler AFB, MS
logsa	AMC, LOGSA	Army Materials Command, VA
msc	MSC	Military Sealift Command, Navy Yard, DC
mtmc	MTMC	ARMY Military Traffic Management Command, VA
navcent-dep	NAVCENT (REAR)	Navy Central Command Rear, MacDill AFB, FL
naveur	NAVEUR	Navy, Europe, Eng. (EUCOM)
navso	NAVSO	Navy Southern, VA (SOUTHCOM)
navspace	NAVSPACE	Navy Space Command, VA
ndu	NDU	National Defense University, Ft. McNair, DC (JOINT)
nmcc	NMCC	National Military Command Center, Pentagon (DISA)
nps	NPS	Naval Post Graduate School, Monterey, CA
nwc	NWC	Naval War College, RI
osf	OSF	Operational Support Facility, Sterling, VA (DISA)
pacaf	PACAF	Air Forces, Pacific, Hickam AFB, HI
pacom	PACOM	Pacific Command, Camp Smith, HI (JOINT)
pacom	MARFORPAC	Marine Forces, Pacific Command, Camp Smith, HI
pacom	MARFORCENT	Marine Forces, Central Command, Camp Smith, HI
pacom	SOCPAC	Special Operations Command (PACOM), Camp Smith, HI
pacflt/*crf*	PACFLT	Pacific Fleet, Makalapa (Navy)
socom	SOCOM	US Special Operations Command, MacDill AFB, FL (AF)
>>socsouth	SOCSOUTH	Special Operations Command (SOUTHCOM), Ft Clayton, Panama
soeur	NAVSOTHEUR	Navy, Southern Europe, Naples, Italy
southaf	SOUTHAF	Air Force Southern Command, Davis-Monthan AFB, AZ
southcom	SOUTHCOM	US Southern Command, Quarry Heights, Panama (Army)
spacecom	SPACECOM	US Space Command, Peterson AFB, CO (JOINT)
speccom	SPECWARCOM (NAV)	Special Warfare Command, CA (Navy)
sstm	SSTM	(AETC), Keesler, MS
stratcom	STRATCOM	US Strategic Command, Offutt AFB, Nebraska
usafe	USAFE	US Air Forces, Europe, GE
usfj	COMUSJAPAN	Commander US Forces Japan (AF)
usfk	USFK/Army(2)	Commander US Forces Korea, Korea (ARMY)
usfk	USFK/Army(1)	Army, Korea
usfk	USFK/Army(3)	Army, Korea

Table 5-1. Domain Names (con't)

GCCS SUBDOMAIN NAME/*alias*	**COMMAND**	**ADDRESS (CONTAINS S/A DESIGNATION)**
ustc	TRANSCOM	US Transportation Command, Scott AFB, IL
ustc	JTO	Joint Training Organization, Scott AFB, IL
	DISA-EUR	DISA Europe, GE
	DISA-PAC	DISA Pacific, HI
	NCC	National Control Center, Pentagon (DISA)
	NMC	National Monitoring Center, Arlington, VA (DISA)

Italics - Alias

To update or correct this table, contact:
Mary Jane Haley
(703)- 735-8587
DSN - 652-8587
e-mail - *haleym@cc.ims.disa.mil*
SIPRNET e-mail - *haleym@hornet.osf.gcc.smil*

5.4 Installing the Primary Name Server

WARNING: Be very careful of the syntax and location of white space and "." in these files; they must be exact or they will not work and the installer will not receive a clear indication of failure. There are four important, but easily overlooked, syntactical errors that can occur:

a. There must be a dot at the end of the fully qualified names; e.g.,

hornet.osf.gcc.smil.

The final dot lets DNS know to start at the root server.

b. Make sure there are no uncommented white lines or the file will not be fully read. Comments in these files are noted by a semi-colon (**;**) at the beginning of each comment line.

c. The *db.hosts*, *db.rev.hosts*, and *db.local* files have a serial number in their files. This number needs to be incremented each time these files are edited. If the site does not increment this number, the DNS daemon will not know there has been a change and will not read any edits. This problem will be discovered when the edited file is chosen.

d. The *db.cache* file has a "dot" at the beginning of the lines that identify the root name servers. DNS will not function properly without the dots.

The following files are located in / *var*/*nameserver*.

NOTE: These are examples and must be modified for the site.

`db.hosts`	Maps local domain names and aliases to addresses.
`db.rev.hosts`	Maps addresses to local domain names.
`db.cache`	Root name server address locations.
`db.local`	Loopback network.
`named.boot`	Ties all the other files together.

NOTE: These files are generally referred to as the name server database (*db.xxx*) files and can have any name the site chooses.

a. Set up the *db.hosts* file. This file, with the *db.rev.hosts* file, defines the domain for which a site's name server is authoritative (the best source of information). It contains the following types of records:

SOA	Start of authority is always the first entry. There can be only one in a database file.
NS	Lists a name server for this domain.
A	Maps a name to an address.
CNAME	Defines an alias (called a canonical name).
PTR	Maps an address to a name.
MX	Mail Exchanger defines a mail hub for the local network.

NOTE: This list is not an exhaustive list of all available record types. It supplies enough to begin setting up the file.

The following is a sample *db.host* file:

NOTE: A semi-colon (;) indicates a comment.

```
;
; Name Server tables for the server at jdef.gcc.smil
;
; Last update Wed Mar 10 20:16:33 1993
;
@  IN SOA    backfire.jdef.gcc.smil. root.backfire.jdef.gcc.smil. (
      93051013        ; serial number
      3600            ; refresh after 1 hour
      300             ; retry after 5 minutes
      604800          ; expire after 1 week
             3600 )       ; minimum time to live (ttl) of 1
                          ; hour
jdef.gcc.smil.  IN NS     backfire.jdef.gcc.smil.
                IN NS     jdef1000.jdef.gcc.smil.
$ORIGIN jdef.gcc.smil.
backfire     IN A         199.114.66.86
mailhost     IN CNAME backfire.jdef.gcc.smil.
jdefrouter   IN A         199.114.66.90
jdef1000     IN A         199.114.66.80
GCCS_SRV     IN CNAME jdef1000.jdef.gcc.smil.
UCCS_SRV     IN CNAME jdef1000.jdef.gcc.smil.
uccs_server  IN CNAME jdef1000.jdef.gcc.smil.
gsorts       IN CNAME backfire.jdef.gcc.smil.
jws3         IN A         199.114.66.70
jots1        IN A     199.114.66.89
localhost    IN A         127.0.0.1
;
```

NOTE: The dot (".") at the end of a fully qualified name means to start at the root domain.

When a record is changed in a database file, the corresponding serial number should always be incremented. Having made this change, the name server daemon can then be signaled to check the database and update its records and the secondary name server's records. A good practice is to use the date and time the serial the number in *YYMMDDHH* format.

The *root.jdef.gcc.smil.* is the mail address for the person responsible for this domain.

b. Set up the *db.rev.hosts* file. Because addresses are looked up as names in DNS, addresses must also be provided to name mappings. Each host in the domain must have at least one record. The addresses are reversed with *in-addr.arpa* appended. The following is an example of the *db.rev.hosts* file:

```
;
```

```
; Last update Fri Jun 24 10:40:23 1994
;
@   IN SOA   backfire.jdef.gcc.smil.  root.backfire.jdef.gcc.smil.(
      93051013            ; serial number
      3600                ; refresh after 1 hour
      300                 ; retry after 5 minutes
      604800              ; expire after 1 week
      3600 )              ; minimum time to live -
                          ;(ttl) of 1 hour

      IN NS       backfire.jdef.gcc.smil.
      IN NS       jdef1000.jdef.gcc.smil.
$ORIGIN 66.114.199.in-addr.arpa.
86        IN PTR      backfire.jdef.gcc.smil.
80        IN PTR      jdef1000.jdef.gcc.smil.
90        IN PTR      jdefrouter.jdef.gcc.smil.
70        IN PTR      jws3.jdef.gcc.smil.
89        IN PTR      jots1.jdef.gcc.smil.
;
```

c. Set up the *db.cache* file. The name server daemon uses the cache information to resolve an address outside its local domain. The cache points to the primary and secondary root name servers, *hornet.osf.gcc.smil* and *milo.osf.gcc.smil*, respectively. These name servers are located at the OSF and are aware of all the other name servers in the network. An alternate root name server is needed to protect against an OSF site failure. Sites that would like to volunteer to provide this service should mail to " *netadm@osf.gcc.smil*". The *db.cache* file should look exactly like the following:

```
;
;Initial cache of rootservers
;
.            99999999     IN    NS HORNET.OSF.GCC.SMIL.
.            99999999     IN    NS MILO.OSF.GCC.SMIL.
.            99999999     IN    NS HQPAC.PACOM.GCC.SMIL.
.            99999999     IN    NS ARCENT.FORSCOM.GCC.SMIL.
;
;and their addresses

HORNET.OSF.GCC.SMIL.         99999999  IN A  199.114.100.20
MILO.OSF.GCC.SMIL.           99999999  IN A  199.144.100.15
HAPAQ.PACOM.GCC.SMIL.        99999999  IN A  157.223.1.101
ARCENT.FORSCOM.GCC.SMIL.     99999999  IN A  164.222.10.1
```

When an alternate root name server is defined, it will be added here.

d. Set up the *db.local* file. This file provides the loopback address. The following is an example of this file:

```
;
; name.local for jdef
;
$ORIGIN jdef.gcc.smil.
@  IN SOA   backfire.jdef.gcc.smil. root.backfire.jdef.gcc.smil.(
             93051013        ; serial number
             3600            ; refresh after 1 hour
             300             ; retry after 5 minutes
             604800          ; expire after 1 week
             3600 )          ; minimum time to live (ttl) of 1 hour
;
   IN NS     backfire.jdef.gcc.smil.
   IN NS     jdef1000.jdef.gcc.smil.
1  IN PTR    localhost.
;
; So much for wraparound 127.0.0.1
;
```

e. Set up the *named.boot* file. This file ties all of the database files together. It specifies the catalog where the database files reside, and the file name the site has chosen for each database. The following is an example of the *named.boot* file:

```
;
; named.boot for primary name server for your domain
;
;type        domain                     sourcefile or host
;
directory    /var/nameserver
cache        .                          db.cache
primary      jdef.gcc.smil              db.hosts
primary      66.114.199.in-addr.arpa    db.rev.hosts
primary      0.0.127.in-addr.arpa       db.local
;
```

When all the database files and the *named.boot* file are completed, copy the *named.boot* file to /*etc*/*named.boot* directory:

```
# cp /var/nameserver/named.boot /etc/named.boot<return>
```

To start the name server daemon, as **root** enter:

```
# in.named<return>
```

During system startup, if the / *etc*/*named.boot* file exists, the *in.named* daemon will be automatically started.

f. Set up the /*etc*/*resolv.conf* file. This file defines the name servers for a domain. Set it up as follows:

```
domain yourdomain.gcc.smil<return>
nameserver ip_address_of_primary_name_server<return>
nameserver ip_address_ of_secondary_name_server<return>
nameserver ip_address_of _offsite_backup_name_server<return>
```

Be sure there are no extra lines or spaces at the end of a line. If there are extra spaces, the resolver does not work, and it does not provide any error messages. For devices in a domain that are not name servers, this is the pathway to a name server. A maximum of three name servers may be listed in the resolver.

g. Perform the following steps to complete the installation:

1. Verify that the / *etc*/*defaultrouter* file contains the IP address for the site's gateway. If this file does not exist, or contains the wrong value, create it and add the IP address of the default gateway.

2. To dynamically set the default gateway, type:

   # **route add net default <IP_address> 1**<return>

3. Verify the netmasks using the "ifconfig" command:

   # **ifconfig le0**<return>

The following is an example of a Class B network with a Class C netmask:

```
le0 : flags = 863<up , broadcast , notrailers , running , multicast > mtu 1500
      inet 164.117.210.77 netmask . ffffff00 broadcast 164.117.210.255
```

NOTE: 164.117.210.77 should be your host's IP address.

("Netmask" should be ffff0000 if Class B netmask is desired. It should match A.2.

"Broadcast" should be 164.117.255.255 if Class B network is desired.)

4. To update a non-NIS system, edit / *etc*/*netmasks* and enter the command:

   # **ifconfig -a netmask + broadcast +**<return>

5.5 Secondary Name Server Setup

a. Create a catalog like / *var*/*nameserver* like the primary name server. Touch the *db.hosts* and *db.rev.hosts* files as follows:

```
# mkdir /var/nameserver<return>
# cd /var/nameserver<return>
# touch db.hosts db.rev.hosts<return>
```

b. Create or copy the *named.boot*, *db.cache*, and *db.local* files from the primary server. In the *named.boot* file, change every occurrence of primary to secondary except for the *db.local* entry.

For the *db.hosts* and *db.rev.hosts* files, add the IP address of the primary server. The file should be similar to the following:

```
;
; Secondary (backup) nameserver
;
;type          domain                    sourcefile or ip address
;
directory      /var/nameserver
cache          .                         db.cache
secondary      jdef.gcc.smil             199.114.66.86 db.hosts
secondary      66.114.199.in-addr.arpa   199.114.66.86 db.rev.hosts
primary        0.0.127.in-addr.arpa      db.local
;
```

Copy the file to /*etc*/*named.boot* and start the name server daemon.

5.6 Set Up the Remaining Hosts on the Network

The remaining hosts use the /*etc*/*resolv.conf* file to locate the name servers for a domain. Set up the remaining hosts as follows:

domain {your domain} **.gcc.smil**
nameserver {ip_address_of_primary_name_server}
nameserver {ip_address_of_secondary_name_server}
nameserver {ip_address_of_offsite_backup_name_server}

Be sure there are no extra lines or spaces at the end of a line. If there are extra spaces, the resolver does not work, and it does not provide any error messages. A maximum of three name servers may be listed in the resolver.

5.7 Debugging Hints

- If the *in.named* daemon does not start:

  First check the /*var*/*adm*/*messages* file. An error message is printed there if *syslog* is turned on.

- If things are not working as expected:

  Check the cache by signaling the *in.named* daemon as follows:

  # **kill -INT `cat /etc/named.pid`**<return>

  This will cause a dump to the /*var*/*tmp*/*named_dump.db* file.

- The *nslookup* facility provides insight into how DNS sees the network. Enter the command **`nslookup`** and use help to get a list of available options.

5.8 Updating the Name Server Database

Edit the files as appropriate, making sure to increment the serial number (always edit the files on the primary). Signal the *in.named* daemon of the change, using the following command. This command will insert the process ID (pid) of the named daemon as an argument for the kill command (HUP is the UNIX signal name for Hangup):

```
    kill -HUP `cat /etc/named.pid`<return>
```

Force an update of the secondary name server using the following command:

```
usr/sbin/in.named -xfer -z jdef.gcc.smil -f db.hosts -s 0 backfire.jdef.gcc.smil
<return>
```

NOTE: Substitute site-specific information for " `backfire.jdef` ".

z = the zone
f = the database to update
s = the serial number on the secondary server is the same as the # on the primary server.

If the above command does not work, do the following on the secondary name server: kill the *in.named* daemon, remove the *db.hosts* and *db.rev.hosts* from the secondary, touch the *db.hosts* and *db.rev.hosts* files, then restart the daemon. These actions force an update.

5.9 Solaris 2.3 Specifics

Make sure the /*etc/nsswitch.conf* file reflects DNS resolution. Typically the host map should be like the following:

```
files dns nisplus [NOTFOUND=return]    if running nis+
files dns [NOTFOUND=return]            if not running nis+
```

NOTE: "files" has been placed first for those sites that have "hot standby" ORACLE database servers. If the primary database server goes down, the site only has to update the */etc/inet/hosts* file to activate the backup.

SECTION 6. NIS+ ADMINISTRATION

6.1 Overview of NIS+

NIS+ is generally required for GCCS Version 2.1, but the decision to implement it is strictly based on site requirements. Host name resolution for GCCS is provided by DNS, and user validation and authentication services can be handled through the / *etc*/*passwd*, /*etc*/*shadow*, and /*etc*/*group* files.

To access other machines across a TCP/IP network, the mnemonic name for the local host must be translated into a numerical value corresponding to the IP number. Three different mechanisms exist within SunOS 5.3 for resolving host name mnemonics into IP numbers: the flat file /etc */hosts*, Domain Name Service (DNS), and Network Information Services (NIS+). Both an / *etc*/*hosts* file and DNS are required for operation of GCCS.

NIS+ provides the capability of maintaining a centralized database of information and making it available to all systems attached to the LAN. For GCCS, this information includes user names, group account information and credentials, and the host names of systems. The basic definitions that a user will require to understand NIS+ are given in Table 6-1.

Table 6-1. NIS+ Definitions

Item	Definition
Domain	A set of machines and the information that is served to those machines.
Client	A process or machine that sends requests for information to the network.
Server	A process that gets client process requests, looks up requested information in a database, and returns the information to the client process.
Master Server	Contains the master set of database information in the form of tables. Updates and additions are made to these tables and are automatically pushed to the replica servers.
Replica Server	Maintains copies of the database tables. These servers are used to distribute the burden of answering client requests and provide backup sources of information in the event the master server is down.

For the purpose of this document, a domain is a set of computers attached to a LAN that share the same administrative information and the shared information itself. Every domain is served by one master server and may have zero or more replica servers. The following instructions define how to install NIS+ on master and replica servers, and the steps necessary to attach clients to them.

6.1.1 The NIS+ Namespace. The arrangement of information stored by the NIS+ is known as the "NIS+ namespace." Although the namespace can be arranged in a variety of ways to suit a specific organization, all sites use the same structural components: directories, tables, and groups. These components are called NIS+ objects. NIS+ objects can be arranged into a hierarchy that resembles a UNIX filesystem but with a number if differences:

- Although both UNIX and NIS+ both use directories, the other objects in a NIS+ namespace are tables and groups, not files.
- The NIS+ namespace is administered only through NIS+ administration commands designed for that purpose; it cannot be administered with standard UNIX filesystem commands.
- The names of UNIX filesystem components are separated by slashes, while the NIS+ namespace objects are separated by dots.
- A UNIX filesystem is traversed from right to left while the NIS+ namespace is reached by traversing from left to right.

NIS+ directories are designed to hold other directories, tables, and groups. Any NIS+ directory that stores groups is named *group_dir* and any directory that stores tables is named *org_dir*. NIS+ directories are normally arranged in configurations called "domains," which are designed to support separate portions of the namespace.

A NIS+ domain consists of a directory object, its *org_dir* directory, its *groups_dir* directory, and a set of NIS+ tables. The instructions for setting up the GCCS domain are contained are the document "GCCS Implementation Procedures."

The NIS+ domain is supported by a NIS+ server, which stores the domain's directories, groups, and tables. It answers requests for access from users, administrators, and applications. A NIS+ client is a workstation that has been set up to receive NIS+ service. Setting up a NIS+ client consists of establishing security credentials, making the client a member of the proper NIS+ groups, verifying its home domain, verifying its Switch configuration file, and running its NIS+ initialization utility.

6.1.2 NIS+ Tables. NIS+ stores information in 16 preconfigured tables that approximate files contained in the UNIX /*etc* directory. The tables are: *Host*, *Bootparams*, *Passwd*, *Cred*, *Group*, *Netgroup*, *Mail_Aliases*, *Timezone*, *Networks*, *Netmasks*, *Eithers*, *Services*, *Protocols*, *RPC*, *Auto_Home* and *Auto_Master*. The current release of GCCS uses only four of these tables: *Host*, *Passwd*, *Groups,* and *Cred*. Different from UNIX files, these tables have a column and entry (row) structure that stores data that can be accessed in multiple ways. These tables cannot be accessed by standard UNIX commands, but rather with a suit of NIS+ commands, most beginning with *nis* that allow access to information contained within the NIS+ tables.

6.1.3 The NIS+ Security. The security features of NIS+ are provided by two means: "authentication" and "authorization." Authentication is the process by which a NIS+ server identifies a NIS+ user or client workstation, known as a "principal," who sent a particular request. Authorization is the process by which a server identifies the access rights granted to a principal. Presently, authentication is the most significant portion of the process used by GCCS.

Authentication is the means by which a NIS+ server verifies the "credentials" of a NIS+ principal. GCCS uses the DES credential type. DES credential information can be stored only in the *Cred* table of the principal's home domain. For GCCS, the home domain is on the EM server, which also contains the NIS+ server. The DES credential is a complex component of NIS+ because of the information it contains and the process involved in creating and verifying it.

The DES credential can be thought of as consisting of the actual credential and the "information" component used to create and verify it. The credential component is the actual item that is sent by the client to the server; the information component is the data stored in the *Cred* table. That information is used for two purposes: it is used by the client to generate the credential and it is used by the server to verify the credential.

The DES credential consists of a principal's secure RPC netname and a verification field. The secure RPC netname portion is the part used to actually identify the NIS+ principal. It is important to note that when the principal is a client user, part of the name is the user's UID; when it is a client workstation, it is the workstation's name. The last field is the principal's home domain.

The verification field of the credential is used to make sure the credential is not forged. It is generated by the "information" component of the process.

Credentials for NIS+ principals can be generated any time after the NIS+ server is created on the EM server. Creating credentials is done using the *nisaddcred* command. It goes through a two-part process: forming the principal's secure RPC netname, and generating the principal's private and public keys, which are their encryption and decryption keys. This is a complex process requiring the principal's network password. From this password, the *nisaddcred* command generates a pair of random, but mathematically related, 192-bit authentication keys, using a special cryptographic scheme. The public key is placed in the "Public Data" field of the *Cred* Table. The private key is placed in the "Private Data" field, but only after being encrypted with the principal's network password.

When a NIS+ client sends a request to a NIS+ server, it sends its DES credential. To generate its DES credential, the client depends on the *keylogin* command, which gives the client access to its private key, since the command fetches the principal's private key from the *Cred* table, decrypts it with the principal's network password, and stores it locally for future requests. The client also needs the public key of the server, which is stored in the client's directory cache. The client then forms the verification field of the credential using the client's private key and the server's public key. It also includes a timestamp, which it also encrypts.

To decrypt the DES credential, the server essentially reverses the encryption process performed by the client.

Problems can arise even if all these activities are performed correctly, due to the existence of old versions of a server's public key. This can be corrected by running *nisupdkeys*.

Authorization defines access rights to the type of operation that NIS+ principals can perform on a NIS+ table or field. Presently, minimum use of this feature exists in GCCS.

6.1.4 Name Service Switch. The Name Service Switch allows NIS+ clients to obtain their network information from one or more sources: NIS+ tables, DNS Host table, or *local* /*etc* files. The choice is determined by consulting the *nsswitch.conf* file, which lists 15 types of information and the locations and order in which to search. The Name Service Switch service searches each location, in order. When it finds a match, it stops searching. If a match is not found, a status message is returned.

6.1.5 Executive Manager Interaction with NIS+. The GCCS Executive Manager is the primary interface with NIS+. The EM's Security Manager creates groups, users, passwords, and formats the result in a form required to input data into the NIS+ tables. The EM's Security Manager also stores them in files located in /*h*/*EM*/*nis_files*. The Executive Manager uses the NIS+ command *nispopulate* to update the NIS+ tables using those files.

6.2 Installing NIS+

6.2.1 Set Up NIS+ on the Executive Manager Server

NOTE: This NIS+ server must be the Executive Manager server.

a. Log on to the system as **root**.

b. Remove any old NIS+ setup files:

```
# cd /var/nis <return>
# rm -rf * <return>
```

c. Remove any references to the default domain:

```
# cd /etc<return>
# rm -f defaultdomain <return>
# rm -f .rootkey <return>
```

d. Kill the processes / *usr*/*sbin*/*rpc.nisd* and /*usr*/*sbin*/*nis_cachemgr*, if they are running:

```
# ps -ef | grep nis <return>
```

Note the process id (PID) for:

/*usr*/*sbin*/*rpc.nisd -r*
/*usr*/*sbin*/*nis_cachemgr*

```
# kill -9 PID <return>
      where PID is the process id for / usr/sbin/rpc.nisd -r
# kill -9 PID <return>
   where PID is the process id for / usr/sbin/nis_cachemgr
```

e. Update the files for NIS+:

```
# cd /h/EM/nis_files <return>
```

Make any necessary updates to the NIS+ source files. In particular, look at the following:

hosts - Enter IP addresses and host names of all systems that are part of the NIS+ environment on the local area network. Syntax for this file is the same as */etc/hosts*. Do not put any aliases in this file.

passwd - Make sure *secman* is the only user when installing on a new system for the first time.

shadow - Make sure *secman* is the only entry user when installing on a new system for the first time.

group - Insure "gccs" and "admin" groups are defined.

f. Change the Group ID on all the files:

```
# chgrp 101 * <return>
# chown root * <return>
```

g. Make sure only owner and group have read/write permission:

```
# chmod 664 passwd group hosts shadow <return>
```

h. Start and configure NIS+ server:

```
# sh<return>
# PATH=$PATH:/usr/lib/nis; export PATH<return>
# nisserver -r -d {Enter the NIS DOMAINNAME}.<return>
```

```
This script sets up this machine "rootmaster" as a NIS+ Root master
Server for domain {NIS DOMAINNAME}.  The following will be displayed
on the screen:

Domainname          : {NIS DOMAINNAME}
NIS+ Group          : admin.{NIS DOMAINNAME}
YP compatibility    : OFF
Security level      : 2=DES

Is this information correct? {Y or N}

Use nisclient -r to restore your current network service environment.

Do you want to continue? {Y or N}
```

If YP compatibility is set to ON answer **N**. If YP compatibility is set to OFF, answer **Y**; and set YP Compatibility to **OFF** when asked.

```
   # Enter login password: {Enter the root password.}<return>
```

i. Populate NIS+ tables from files:

```
# nispopulate -F -p /h/EM/nis_files -d {Enter the NIS DOMAINNAME}.<return>
         # Is info correct? y <return>

         # Do you want to continue? y<return>    (ignore warning on netgroup)

         # cp /h/EM/systools/nsswitch.EM /etc/nsswitch.conf<return>
            # cd /etc <return>
            # vi nsswitch.conf<return>
```

Ensure the entries for *passwd*, *group*, and *hosts* look like the following:

```
   passwd:   nisplus files
   group:    nisplus files
   hosts:    files dns nisplus [NOTFOUND=return]
```

Comment out any other lines with *group*, *passwd*, or *hosts*.

```
   # cat /etc/defaultdomain<return>
```

If it contains the correct domain name, re-boot the system; otherwise do the following:

```
   # echo {NIS DOMAINNAME} > /etc/defaultdomain<return>
```

Re-boot the server:

```
   # init 6<return>
```

j. To add the *secman* account to the NIS+ domain created above, execute the following after logging on to the system as **root**:

```
   # niscat passwd.org_dir<return>
```

Insure that an entry exists for *secman*.

Set the password for *secman*:

```
   # su - secman<return>
   # /usr/lib/nis/nisclient -u<return>
```

When prompted for SECURE-RPC password, enter **nisplus**. When prompted for user's password, enter the user's new password.

```
   # exit <return>
```

k. Additional users may be added to the NIS+ "admin" group. Anyone assigned to this group will be allowed to administer the NIS+ database:

```
# nisgrpadm -a admin.{Enter the NIS DOMAINNAME} .{Enter the USER} .{Enter
the NIS DOMAINNAME} .<return>
```

(Substitute the user's login name that will be added to the "admin" group. This command will give that individual permission to add and delete accounts.)

l. After the NIS+ server has been initialized, execute the following as **root**:

```
nischmod n+r passwd.org_dir<return>
```

6.2.2 Set Up NIS+ on Replica Server. *Replica Services* provide limited utility to GCCS. Backup and mirroring provide better means for maintenance.

6.2.3 Set Up NIS+ on Client

a. Log in to the NIS+ master server (NIS+ must be running).

b. Add the client to the NIS+ host table:

```
# cd /h/EM/nis_files<return>
# vi hosts <return>
  G<return>           (Go to last line of file.)
  o<return>      (Add a new line.)
    {IPnumber} {CLIENT1}<return>
 <ESC> dd       (Exit from insert mode and delete last blank line.)
  :wq <return>
# /usr/lib/nis/nispopulate -F hosts <return>
```

The computer should respond with the following:

```
NIS+ Domainname       : {DOMAINNAME}
Directory Path     : (current directory)

Is this information correct? (Y or N)    Y <return>
```

c. Log in as **root** to the client.

d. Add the {NIS+ MASTER} to / *etc*/*hosts*, if required:

```
# vi /etc/hosts<return>
G<return>             (Go to last line in file.)
o<return>             (Add a new line.)
     {IPaddr} {MASTER} <return>
```

```
<Esc>dd <return>
   :wq!<return>
```

e. Remove any old NIS+ information (if it exists):

```
# rm /etc/.rootkey <return>
# rm -rf /var/nis/*<return>
# rm -rf /etc/defaultdomain<return>
```

f. Initialize the client:

```
# nisclient -i -d {NIS DOMAINNANE} -h {NIS MASTER SERVER}<return>
```

The following appears on the screen:

```
Enter server (servers name) IP address:     {IP Address of server}<return>
Please enter the network password that your administrator gave you.     {password}
<return>
Please enter the secman RPC password for root:     nisplus<return>
Please enter the login password for root: {enter root password}<return>
```

NOTE: Error messages concerning / *etc*/*defaultdomain* should be ignored.

```
# Enter login password:   {enter root password}<return>
```

g. Assign the client to the NIS+ domain:

```
# domainname {NIS DOMAINNAME}<return>
# domainname > /etc/defaultdomain<return>
```

h. Check the client's / *etc*/*nsswitch.conf* file:

```
cp /h/EM/systools/nsswitch.EM    /etc/nsswitch.conf<return>

   # cd /etc <return>
   # vi nsswitch.conf<return>
```

Ensure the entries for *passwd*, *group*, and *hosts* look like the following:

```
passwd:  nisplus files
group:   nisplus files
hosts:   files dns nisplus [NOTFOUND=return]
```

Comment out any other lines with *group*, *passwd*, or *hosts*.

i. Re-boot:

```
# cd /<return>
# init 6<return>
```

SECTION 7. MAIL ADMINISTRATION

7.1 Introduction

Sendmail implements a general purpose internetwork mail routing facility under the UNIX operating system. It is not tied to any one transport protocol. Its function may be likened to a crossbar switch, relaying messages from one domain into another. In the process, it can do a limited amount of message header editing to put the message into a format that is appropriate for the receiving domain. All of this is done under the control of a configuration file.

Due to the requirements of flexibility for *sendmail*, the configuration can seem somewhat unapproachable. However, for most GCCS SIPRNET sites, the only difference in the *sendmail.cf* file is the domain name. Those sites having unique address resolution rules will have to address those individually.

The GCCS COE Kernel tape configures each platform for mail according to how certain questions are answered.

a. If it was stated that the platform is a mail server (mail host) during the installation of the GCCS COE Kernel (see Section 4.3 of the *GCCS Implementation Procedures*), the following occurs:

   1. A preconfigured *main.cf* file[*] is configured with the site's domain name and copied into the /*etc*/*mail*/*sendmail.cf* file.

   2. An alias of *mailhost* is added after the site's host name in the / *etc*/*host* file.

   3. The file system / *var*/*mail* is exported.

b. If it was stated that the platform is <u>not</u> a mail server, the following occurs:

   1. The preconfigured *subsidiary.cf* file is configured with the site's domain name and copied into the /*etc*/*mail*/*sendmail.cf* file.

   2. An IP address with an alias of *mailhost* is added to the host table of that platform.

   3. The /*var*/*mail* file system of the mail server is mounted.

c. The /*usr*/*lib*/*sendmail.mx* file is copied to / *usr*/*lib*/*sendmail* to enable mail to use DNS.

[*] Copies of these mail administration files are provided in Section 7.2, with bold print used to identify fields that were modified.

Although *sendmail* is intended to run without the need for monitoring, it has a number of features that may be used to monitor or adjust the operation under unusual circumstances. These features are not described in this document. The following list of documents are recommended for those who would like more detailed information on the operation of sendmail:

sendmail, by Bryan Costales with Eric Allman & Neil Rickert,
published by O'Reily & Associates.

sendmail - An Internetwork Mail Router, by Eric Allman (SMM-16)

sendmail - Installation and Operation Guide, by Eric Allman (SMM-07).

Other useful documents are the following Requests for Comments (RFCs):

RFC822	Standard for the Format of ARPA-Internet Text Messages
RFC821	Simple Mail Transfer Protocol
RFC819	The Domain naming Convention for Internet User Applications
RFC1123	Requirements for Internet hosts - Application and Support.

To receive these RFCs via electronic mail:

```
mail service@rs.internic.net
help
```

or

```
mail service@rs.internic.net
send RFC 822
```

7.2 Mail Administration Files

```
############################################################
#
#       Sendmail configuration file for "MAIN MACHINES"
#
#       You should install this file as /etc/sendmail.cf
#       if your machine is the main (or only) mail-relaying
#       machine in your domain.  Then edit the file to
#       customize it for your network configuration.
#
#       See the manual "System and Network Administration for the Sun
#       Workstation". Look at "Setting Up The Mail Routing System" in
#       the chapter on Communications.  The Sendmail reference in the
#       back of the manual is also useful.
#
#       @(#)main.mc 1.17 90/01/04 SMI
#

###     local info
```

```
# delete the following if you have no sendmailvars table
Lmmaildomain

# my official hostname
# You have two choices here.  If you want the gateway machine to identify
# itself as the DOMAIN, use this line:
Dj$m
# If you want the gateway machine to appear to be INSIDE the domain, use:
#Dj$w.$m
# if you are using sendmail.mx (or have a fully-qualified hostname), use:
#Dj$w

# major relay mailer - typical choice is "ddn" if you are on the
# Defense Data Network (e.g. Arpanet or Milnet)
#DMsmartuucp
DMddn

# major relay host: use the $M mailer to send mail to other domains
#DR ddn-gateway
#CR ddn-gateway
DR mailhost
CR mailhost


# If you want to pre-load the "mailhosts" then use a line like
# FS /usr/lib/mailhosts
# and then change all the occurrences of $%y to be $=S instead.
# Otherwise, the default is to use the hosts.byname map if NIS
# is running (or else the /etc/hosts file if no NIS).

# valid top-level domains (default passes ALL unknown domains up)
CT arpa com edu gov mil net org   smil
CT us de fr jp kr nz il uk no au fi nl se ca ch my dk ar

# options that you probably want on a mailhost:

# checkpoint the queue after this many recipients
OC10

# refuse to send tiny messages to more than these recipients
Ob10

#################################################
#
#     General configuration information

# local domain names
#
# These can now be determined from the domainname system call.
# The first component of the NIS domain name is stripped off unless
# it begins with a dot or a plus sign.
# If your NIS domain is not inside the domain name you would like to have
# appear in your mail headers, add a "Dm" line to define your domain name.
# The Dm value is what is used in outgoing mail.  The Cm values are
# accepted in incoming mail.  By default Cm is set from Dm, but you might
# want to have more than one Cm line to recognize more than one domain
# name on incoming mail during a transition.
# Example:
# DmCS.Podunk.EDU
# Cm cs cs.Podunk.EDU
#

DmDUMMY.
Cm DUM DUMMY.

# known hosts in this domain are obtained from gethostbyname() call

# Version number of configuration file
#ident    "@(#)version.m4    1.17   92/07/14 SMI"   /* SunOS 4.1    */
#
#
#         Copyright Notice
#
#Notice of copyright on this source code product does not indicate
#publication.
#
#     (c) 1986,1987,1988,1989  Sun Microsystems, Inc
#                All rights reserved.

DVSMI-SVR4


###   Standard macros

# name used for error messages
DnMailer-Daemon
# special user
CDMailer-Daemon root daemon uucp
# UNIX header format
DlFrom $g  $d
# delimiter (operator) characters
Do.:%@!^=/[]
# format of a total name
Dq$g$?x ($x)$.
# SMTP login message
De$j Sendmail $v/$V ready at $b

###   Options

# Remote mode - send through server if mailbox directory is mounted
OR
# location of alias file
OA/etc/mail/aliases
# default delivery mode (deliver in background)
Odbackground
# rebuild the alias file automagically
OD
# temporary file mode -- 0600 for secure mail, 0644 for permissive
OF0600
# default GID
Og1
# location of help file
```

```
OH/etc/mail/sendmail.hf
# log level
OL9
# default messages to old style
Oo
# Cc my postmaster on error replies I generate
OPPostmaster
# queue directory
OQ/var/spool/mqueue
# read timeout for SMTP protocols
Or15m
# status file -- none
OS/etc/mail/sendmail.st
# queue up everything before starting transmission, for safety
Os
# return queued mail after this long
OT3d
# default UID
Ou1

###   Message precedences
Pfirst-class=0
Pspecial-delivery=100
Pjunk=-100

###   Trusted users
T root daemon uucp

###   Format of headers
H?P?Return-Path: <$g>
HReceived: $?sfrom $s $.by $j ($v/$V)
       id $i; $b
H?D?Resent-Date: $a
H?D?Date: $a
H?F?Resent-From: $q
H?F?From: $q
H?x?Full-Name: $x
HSubject:
H?M?Resent-Message-Id: <$t.$i@$j>
H?M?Message-Id: <$t.$i@$j>
HErrors-To:

###########################
###   Rewriting rules   ###
###########################


#  Sender Field Pre-rewriting
S1
# None needed.

#  Recipient Field Pre-rewriting
S2
# None needed.

# Name Canonicalization
# Internal format of names within the rewriting rules is:
#     anything<@host.domain.domain...>anything
# We try to get every kind of name into this format, except for local
# names, which have no host part.  The reason for the "<>" stuff is
# that the relevant host name could be on the front of the name (for
# source routing), or on the back (normal form).  We enclose the one that
# we want to route on in the <>'s to make it easy to find.
#
S3

# handle "from:<>" special case
R$*<>$*                   $@@                       turn into magic token

# basic textual canonicalization
R$*<$+>$*                 $2                        basic RFC822 parsing

# make sure <@a,@b,@c:user@d> syntax is easy to parse -- undone later
R@$+,$+:$+                @$1:$2:$3                 change all "," to ":"
R@$+:$+                   $@$>6<@$1>:$2             src route canonical

R$+:$*;@$+                $@$1:$2;@$3               list syntax
R$+@$+                    $:$1<@$2>                 focus on domain
R$+<$+@$+>                $1$2<@$3>                 move gaze right
R$+<@$+>                  $@$>6$1<@$2>              already canonical

# convert old-style names to domain-based names
# All old-style names parse from left to right, without precedence.
R$-!$+                    $@$>6$2<@$1.uucp>         uucphost!user
R$-.$+!$+                 $@$>6$3<@$1.$2>           host.domain!user
R$+%$+                    $@$>3$1@$2                user%host

#  Final Output Post-rewriting
S4
R$+<@$+.uucp>             $2!$1                     u@h.uucp => h!u
R$+                       $: $>9 $1                 Clean up addr
R$*<$+>$*                 $1$2$3                    defocus


#  Clean up an name for passing to a mailer
#  (but leave it focused)
S9
R$=w!@                    $@$w!$n
R@                        $@$n                      handle <> error addr
R$*<$*LOCAL>$*            $1<$2$m>$3                change local info
R<@$+>$*:$+:$+            <@$1>$2,$3:$4             <route-addr> canonical


#######################
#   Rewriting rules

# special local conversions
S6
R$*<@$*$=m>$*             $1<@$2LOCAL>$4            convert local domain

# Local and Program Mailer specification
```

```
Mlocal,   P=/bin/mail, F=flsSDFMmnP, S=10, R=20, A=mail -d $u
Mprog,    P=/bin/sh,   F=lsDFMeuP,  S=10, R=20, A=sh -c $u

S10
# None needed.

S20
# None needed.

#ident    "@(#)etherm.m4  1.15  93/04/05 SMI"   /* SunOS 4.1    */
#
#         Copyright Notice
#
#Notice of copyright on this source code product does not indicate
#publication.
#
#      (c) 1986,1987,1988,1989  Sun Microsystems, Inc
#                All rights reserved.

############################################################
#####
#####     Ethernet Mailer specification
#####
##### Messages processed by this configuration are assumed to remain
##### in the same domain.  This really has nothing particular to do
#####   with Ethernet - the name is historical.

Mether,   P=[TCP], F=msDFMuCX, S=11, R=21, A=TCP $h
S11
R$*<@$+>$*              $@$1<@$2>$3                  already ok
R$=D                    $@$1<@$w>                    tack on my hostname
R$+                     $@$1<@$k>                    tack on my mbox hostname

S21
R$*<@$+>$*              $@$1<@$2>$3                  already ok
R$+                     $@$1<@$k>                    tack on my mbox hostname



##########################################################
#  General code to convert back to old style UUCP names
S5
R$+<@LOCAL>             $@ $w!$1                     name@LOCAL => sun!name
R$+<@$-.LOCAL>          $@ $2!$1                     u@h.LOCAL => h!u
R$+<@$+.uucp>           $@ $2!$1                     u@h.uucp => h!u
R$+<@$*>                $@ $2!$1                     u@h => h!u
# Route-addrs do not work here.  Punt til uucp-mail comes up with something.
R<@$+>$*                $@ @$1$2                     just defocus and punt
R$*<$*>$*               $@ $1$2$3                    Defocus strange stuff

#      UUCP Mailer specification

Muucp,    P=/usr/bin/uux, F=msDFMhuU, S=13, R=23,
          A=uux - -r -a$f $h!rmail ($u)
```

```
# Convert uucp sender (From) field
S13
R$+                     $:$>5$1                     convert to old style
R$=w!$+                 $2                          strip local name
R$+                     $:$w!$1                     stick on real host name

# Convert uucp recipient (To, Cc) fields
S23
R$+                     $:$>5$1                     convert to old style


#ident   "@(#)ddnm.m4    1.8   93/06/30 SMI"   /* SunOS 4.1    */
#
#
#        Copyright Notice
#
#Notice of copyright on this source code product does not indicate
#publication.
#
#     (c) 1986,1987,1988,1989  Sun Microsystems, Inc
#               All rights reserved.

############################################################
#
#        DDN Mailer specification
#
#     Send mail on the Defense Data Network
#        (such as Arpanet or Milnet)

Mddn, P=[TCP], F=msDFMuCX, S=22, R=22, A=TCP $h, E=\r\n

# map containing the inverse of mail.aliases
# Note that there is a special case mail.byaddr will cause reverse
# lookups in both Nis+ and NIS.
# If you want to use ONLY Nis+ for alias inversion comment out the next line
# and uncomment the line after that
DZmail.byaddr
#DZREVERSE.mail_aliases.org_dir

S22
R$*<@LOCAL>$*             $:$1
R$-<@$->                  $:$>3${Z$1@$2$}          invert aliases
R$*<@$+.$*>$*             $@$1<@$2.$3>$4           already ok
R$+<@$+>$*                $@$1<@$2.$m>$3           tack on our domain
R$+                       $@$1<@$w.$m>             tack on our full name


# "Smart" UUCP mailer: Uses UUCP transport but domain-style naming
Msmartuucp, P=/usr/bin/uux, F=CmsDFMhuU, S=22, R=22,
      A=uux - -r $h!rmail ($u)


############################################################
#
#        RULESET ZERO
#
```

```
#     This is the ruleset that determines which mailer a name goes to.

# Ruleset 30 just calls rulesets 3 then 0.
S30
R$*                      $: $>3 $1                  First canonicalize
R$*                      $@ $>0 $1                  Then rerun ruleset 0

S0
# On entry, the address has been canonicalized and focused by ruleset 3.
# Handle special cases.....
R@                       $#local $:$n               handle <> form

# resolve the local hostname to "LOCAL".
R$*<$*$=w.LOCAL>$*       $1<$2LOCAL>$4              thishost.LOCAL
R$*<$*$=w.uucp>$*        $1<$2LOCAL>$4              thishost.uucp
R$*<$*$=w>$*             $1<$2LOCAL>$4              thishost

# Mail addressed explicitly to the domain gateway (us)
R$*<@LOCAL>              $@$>30$1                   strip our name, retry
R<@LOCAL>:$+             $@$>30$1                   retry after route strip

# For numeric spec, you can't pass spec on to receiver, since old rcvr's
# are not smart enough to know that [x.y.z.a] is their own name.
R<@[$+]>:$*              $:$>9 <@[$1]>:$2           Clean it up, then...
R<@[$+]>:$*              $#ether $@[$1] $:$2        numeric internet spec
R<@[$+]>,$*              $#ether $@[$1] $:$2        numeric internet spec
R$*<@[$+]>               $#ether $@[$2] $:$1        numeric internet spec

# deliver to known ethernet hosts explicitly specified in our domain
R$*<@$%y.LOCAL>$*        $#ether $@$2 $:$1<@$2>$3         user@host.sun.com
# deliver to hosts in our domain that have a MX recod
R$*<@$%x.LOCAL>$*        $#ether $@$2 $:$1<@$2>$3         user@host.sun.com

# etherhost.uucp is treated as etherhost.$m for now.
# This allows them to be addressed from uucp as foo!sun!etherhost!user.
R$*<@$%y.uucp>$*         $#ether $@$2 $:$1<@$2>$3         user@etherhost.uucp

# Explicitly specified names in our domain -- that we've never heard of
R$*<@$*.LOCAL>$*         $#error $:Never heard of host $2 in domain $m

# Clean up addresses for external use -- kills LOCAL, route-addr ,=>:
R$*                      $:$>9 $1                         Then continue...

# resolve UUCP-style names
R<@$-.uucp>:$+           $#uucp    $@$1 $:$2                 @host.uucp:...
R$+<@$-.uucp>            $#uucp    $@$2 $:$1                 user@host.uucp

# Pass other valid names up the ladder to our forwarder
#R$*<@$*.$=T>$*          $#$M      $@$R $:$1<@$2.$3>$4       user@domain.known

# Replace following with above to only forward "known" top-level domains
#R$*<@$*.$+>$*           $#$M      $@$R $:$1<@$2.$3>$4       user@any.domain

# if you are on the DDN, then comment-out both of the the lines above
# and use the following instead:
R$*<@$*.$+>$*            $#ddn     $@ $2.$3 $:$1<@$2.$3>$4   user@any.domain
```

```
# All addresses in the rules ABOVE are absolute (fully qualified domains).
# Addresses BELOW can be partially qualified.

# deliver to known ethernet hosts
R$*<@$%y>$*               $#ether $@$2 $:$1<@$2>$3     user@etherhost
# deliver to known ethernet hosts that has MX record
R$*<@$%x>$*               $#ether $@$2 $:$1<@$2>$3     user@etherhost

# other non-local names have nowhere to go; return them to sender.
R$*<@$+.$->$*             $#error $:Unknown domain $3
R$*<@$+>$*                $#error $:Never heard of $2 in domain $m
R$*@$*                    $#error $:I don't understand $1@$2

# Local names with % are really not local!
R$+%$+                    $@$>30$1@$2        turn % => @, retry

# everything else is a local name
R$+                       $#local $:$1       local names


###########################################################
#
#      SENDMAIL CONFIGURATION FILE FOR SUBSIDIARY MACHINES
#
#      You should install this file as /etc/sendmail.cf
#      if your machine is a subsidiary machine (that is, some
#      other machine in your domain is the main mail-relaying
#      machine).  Then edit the file to customize it for your
#      network configuration.
#
#      @(#)subsidiary.mc 1.11 88/02/08 SMI; from UCB arpa.mc 3.25 2/24/83
#

# delete the following if you have no sendmailvars table
Lmmaildomain

# local UUCP connections -- not forwarded to mailhost
CV

# my official hostname
Dj$w.$m

# major relay mailer
DMddn

# major relay host
DRmailhost
CRmailhost

#################################################
#
#      General configuration information

# local domain names
#
# These can now be determined from the domainname system call.
# The first component of the NIS domain name is stripped off unless
# it begins with a dot or a plus sign.
# If your NIS domain is not inside the domain name you would like to have
# appear in your mail headers, add a "Dm" line to define your domain name.
# The Dm value is what is used in outgoing mail.  The Cm values are
# accepted in incoming mail.  By default Cm is set from Dm, but you might
# want to have more than one Cm line to recognize more than one domain
# name on incoming mail during a transition.
# Example:
# DmCS.Podunk.EDU
# Cm cs cs.Podunk.EDU
#
# known hosts in this domain are obtained from gethostbyname() call

DmDUMMY.
Cm DUM DUMMY.


# Version number of configuration file
#ident    "@(#)version.m4    1.17  92/07/14 SMI"   /* SunOS 4.1    */
#
#
#         Copyright Notice
#
#Notice of copyright on this source code product does not indicate
#publication.
#
#      (c) 1986,1987,1988,1989  Sun Microsystems, Inc
#               All rights reserved.

DVSMI-SVR4


###   Standard macros

# name used for error messages
DnMailer-Daemon
# specail user
CDMailer-Daemon root daemon uucp
# UNIX header format
DlFrom $g  $d
# delimiter (operator) characters
Do.:%@!^=/[]
# format of a total name
Dq$g$?x ($x)$.
# SMTP login message
De$j Sendmail $v/$V ready at $b

###   Options

# Remote mode - send through server if mailbox directory is mounted
OR
# location of alias file
OA/etc/mail/aliases
# default delivery mode (deliver in background)
Odbackground
```

```
# rebuild the alias file automagically
OD
# temporary file mode -- 0600 for secure mail, 0644 for permissive
OF0600
# default GID
Og1
# location of help file
OH/etc/mail/sendmail.hf
# log level
OL9
# default messages to old style
Oo
# Cc my postmaster on error replies I generate
OPPostmaster
# queue directory
OQ/var/spool/mqueue
# read timeout for SMTP protocols
Or15m
# status file -- none
OS/etc/mail/sendmail.st
# queue up everything before starting transmission, for safety
Os
# return queued mail after this long
OT3d
# default UID
Ou1

###   Message precedences
Pfirst-class=0
Pspecial-delivery=100
Pjunk=-100

###   Trusted users
T root daemon uucp

###   Format of headers
H?P?Return-Path: <$g>
HReceived: $?sfrom $s $.by $j ($v/$V)
      id $i; $b
H?D?Resent-Date: $a
H?D?Date: $a
H?F?Resent-From: $q
H?F?From: $q
H?x?Full-Name: $x
HSubject:
H?M?Resent-Message-Id: <$t.$i@$j>
H?M?Message-Id: <$t.$i@$j>
HErrors-To:

###########################
###   Rewriting rules   ###
###########################


#  Sender Field Pre-rewriting
S1
```

```
# None needed.

#  Recipient Field Pre-rewriting
S2
# None needed.

# Name Canonicalization

# Internal format of names within the rewriting rules is:
#     anything<@host.domain.domain...>anything
# We try to get every kind of name into this format, except for local
# names, which have no host part.  The reason for the "<>" stuff is
# that the relevant host name could be on the front of the name (for
# source routing), or on the back (normal form).  We enclose the one that
# we want to route on in the <>'s to make it easy to find.
#
S3

# handle "from:<>" special case
R$*<>$*                  $@@                       turn into magic token

# basic textual canonicalization
R$*<$+>$*                $2                        basic RFC822 parsing

# make sure <@a,@b,@c:user@d> syntax is easy to parse -- undone later
R@$+,$+:$+               @$1:$2:$3                 change all "," to ":"
R@$+:$+                  $@$>6<@$1>:$2             src route canonical

R$+:$*;@$+               $@$1:$2;@$3               list syntax
R$+@$+                   $:$1<@$2>                 focus on domain
R$+<$+@$+>               $1$2<@$3>                 move gaze right
R$+<@$+>                 $@$>6$1<@$2>              already canonical

# convert old-style names to domain-based names
# All old-style names parse from left to right, without precedence.
R$-!$+                   $@$>6$2<@$1.uucp>         uucphost!user
R$-.$+!$+                $@$>6$3<@$1.$2>           host.domain!user
R$+%$+                   $@$>3$1@$2                user%host

#  Final Output Post-rewriting
S4
R$+<@$+.uucp>            $2!$1                     u@h.uucp => h!u
R$+                      $: $>9 $1                 Clean up addr
R$*<$+>$*                $1$2$3                    defocus


#  Clean up an name for passing to a mailer
#  (but leave it focused)
S9
R$=w!@                   $@$w!$n
R@                       $@$n                      handle <> error addr
R$*<$*LOCAL>$*           $1<$2$m>$3                change local info
R<@$+>$*:$+:$+           <@$1>$2,$3:$4             <route-addr> canonical


#######################
```

```
#   Rewriting rules

# special local conversions
S6
R$*<@$*$=m>$*             $1<@$2LOCAL>$4            convert local domain

# Local and Program Mailer specification

Mlocal,   P=/bin/mail, F=flsSDFMmnP, S=10, R=20, A=mail -d $u
Mprog,    P=/bin/sh,   F=lsDFMeuP,  S=10, R=20, A=sh -c $u

S10
# None needed.

S20
# None needed.

#ident    "@(#)etherm.m4  1.15   93/04/05 SMI"   /* SunOS 4.1    */
#
#         Copyright Notice
#
#Notice of copyright on this source code product does not indicate
#publication.
#
#     (c) 1986,1987,1988,1989  Sun Microsystems, Inc
#               All rights reserved.

############################################################
#####
#####     Ethernet Mailer specification
#####
##### Messages processed by this configuration are assumed to remain
##### in the same domain.  This really has nothing particular to do
#####   with Ethernet - the name is historical.

Mether,   P=[TCP], F=msDFMuCX, S=11, R=21, A=TCP $h
S11
R$*<@$+>$*                $@$1<@$2>$3               already ok
R$=D                      $@$1<@$w>                 tack on my hostname
R$+                       $@$1<@$k>                 tack on my mbox hostname

S21
R$*<@$+>$*                $@$1<@$2>$3               already ok
R$+                       $@$1<@$k>                 tack on my mbox hostname



##########################################################
#  General code to convert back to old style UUCP names
S5
R$+<@LOCAL>               $@ $w!$1                  name@LOCAL => sun!name
R$+<@$-.LOCAL>            $@ $2!$1                  u@h.LOCAL => h!u
R$+<@$+.uucp>             $@ $2!$1                  u@h.uucp => h!u
R$+<@$*>                  $@ $2!$1                  u@h => h!u
# Route-addrs do not work here.  Punt til uucp-mail comes up with something.
```

```
R<@$+>$*                  $@ @$1$2                  just defocus and punt
R$*<$*>$*                 $@ $1$2$3                 Defocus strange stuff

#     UUCP Mailer specification

Muucp,    P=/usr/bin/uux, F=msDFMhuU, S=13, R=23,
      A=uux - -r -a$f $h!rmail ($u)

# Convert uucp sender (From) field
S13
R$+                       $:$>5$1                   convert to old style
R$=w!$+                   $2                        strip local name
R$+                       $:$w!$1                   stick on real host name

# Convert uucp recipient (To, Cc) fields
S23
R$+                       $:$>5$1                   convert to old style


#####     RULESET ZERO PREAMBLE

# Ruleset 30 just calls rulesets 3 then 0.
S30
R$*                       $: $>3 $1                 First canonicalize
R$*                       $@ $>0 $1                 Then rerun ruleset 0

S0
# On entry, the address has been canonicalized and focused by ruleset 3.
# Handle special cases.....
R@                        $#local $:$n              handle <> form
# Earlier releases special-cased the [x.y.z.a] format, but SunOS 4.1 or later
# should handle these properly on input.

# now delete redundant local info
R$*<$*$=w.LOCAL>$*        $1<$2>$4                  thishost.LOCAL
R$*<@LOCAL>$*             $1<@$m>$2                 host == domain gateway
R$*<$*$=w.uucp>$*         $1<$2>$4                  thishost.uucp
R$*<$*$=w>$*              $1<$2>$4                  thishost

# arrange for local names to be fully qualified
R$*<@$%l>$*               $1<@$2.LOCAL>$3           user@etherhost

# For numeric spec, you can't pass spec on to receiver, since old rcvr's
# were not smart enough to know that [x.y.z.a] is their own name.
R<@[$+]>:$*               $:$>9 <@[$1]>:$2          Clean it up, then...
R<@[$+]>:$*               $#ether $@[$1] $:$2       numeric internet spec
R<@[$+]>,$*               $#ether $@[$1] $:$2       numeric internet spec
R$*<@[$+]>                $#ether $@[$2] $:$1       numeric internet spec

R$*<$*.>$*                $1<$2>$3                  drop trailing dot
R<@>:$*                   $@$>30$1                  retry after route strip
R$*<@>                    $@$>30$1                  strip null trash & retry


################################################
###  Machine dependent part of ruleset zero  ###
```

```
################################################

# resolve names we can handle locally
R<@$=V.uucp>:$+        $:$>9 $1                First clean up, then...
R<@$=V.uucp>:$+        $#uucp  $@$1 $:$2        @host.uucp:...
R$+<@$=V.uucp>         $#uucp  $@$2 $:$1        user@host.uucp

# optimize names of known ethernet hosts
R$*<@$%l.LOCAL>$*      $#ether $@$2 $:$1<@$2>$3     user@host.here
# local host that has a MX record
R$*<@$%x.LOCAL>$*      $#ether $@$2 $:$1<@$2>$3     user@host.here

# other non-local names will be kicked upstairs
R$+                    $:$>9 $1                     Clean up, keep <>
R$*<@$+>$*             $#$M    $@$R $:$1<@$2>$3     user@some.where
R$*@$*                 $#$M    $@$R $:$1<@$2>       strangeness with @

# Local names with % are really not local!
R$+%$+                 $@$>30$1@$2              turn % => @, retry

# everything else is a local name
R$+                    $#local $:$1             local names

# Ruleset 33 is used in remote mode only
S33
R$+<@$=w.LOCAL>        $1
R$+<@$=w>              $1
R$*<@$+>$*             $#ether $@$k $:$1<@$2>$3     forward to $k
R$+                    $#local $:$1                 local names
```

SECTION 8. PRINTER ADMINISTRATION

8.1 Scope

This section addresses the installation of the SUN NeWSprint product on those SUNservers that must support SUN printers, and the use of the Network Printer Administration Application provided with GCCS Version 2.1.

8.2 Installing NeWSprint on Print Servers

Any SUNserver or SUNstation that has a SUN printer directly attached to it requires NeWSprint to use that printer. GCCS is currently using the following SUN printers: SPARCprinter, NeWSprinter20, and SPARCprinter II. For the SPARCprinter and the NeWSprinter20, NeWSprint is provided on a CD labeled "NeWSprint Version 2.5 revision b." For the SPARCprinter II, NeWSprint is provided on a CD labeled "Printer Manager Software V1.0 for Solaris 2.X." NeWSprint should be installed immediately after the Solaris operating system has been installed. If a site attempts to install it after NIS+ has been activated, it will encounter problems. Prior to installing NeWSprint the site should obtain a NeWSprint font license. Execute the following steps to install NeWSprint:

a. Log on to the print server as **root**.

b. Insert the NeWSprint CD into the CD drive.

   For SPARCprinterII use the CD "Print Manager Software V1.0 for Solaris 2.X."
   For SPARCprinter/NeWSprinter20 use the CD "NeWSprint Version 2.5 revision b."

c. Enter the following commands:

   cd /cdrom/unnamed_cdrom<return>
   cd sp2<return>   for SPARCprinterII only
   ./npcdm<return>

d. A list of options is displayed. Choose **Option 1: Select Application.**

e. A list of options is displayed. Choose the appropriate option.

   SPARCprinter if using SPARCprinter
   NeWSprinter20 if using NeWSprinter20
   SPARCprinterII if using SPARCprinterII
   NeWSprint if just installing NeWSprint software.

f. Another list of options is displayed. Choose **Option 3: Install Application.**

g. A series of questions and directions is displayed. Answer the questions and directions as follows:

```
Question:    Begin Installation (y/n?)
Answer:      y<return>
```

Press space bar two times to read more license information.

```
Question:    Do you want to continue (y/n?)
Answer:      y<return>

Question:    Do you want to install NeWSprint Answerbook (y/n?)
Answer:      y<return>
```

The following item(s) will be be installed in /opt/NeWSprint:

```
NeWSprint

Continue (y/n?)   y <return>

Question:    What name do you want for the printer?
Answer:      {Whatever name you wish for your printer} <return>

Question:    Do you want this printer to be the default printer (y/n?)
Answer:      y or n <return>

Question:    Do you want to install NeWSprint font license (y/n?)
Answer:      y<return>

Question:    Enter NeWSprint font license:
Answer:      Enter the license provided (Reference Section 10.3)
```

NeWSprint is now installed. SUN patch 102113-03 is required to prevent NeWSprint from locking up after printing one job. This patch is placed in */opt* after the *load_patches* script is executed during the loading of the GCCS COE Kernel (Section 4.1 of Implementation Procedures). To install the patch, execute the following:

a. Shut down the print scheduler with the following command (there is no need to be in single-user mode to load this patch):

lpshut<return>

b. Install patch 102113-03 according to the steps in the README.102113-03 file provided with the patch.

/opt/102113-03/installpatch /opt/102113-03<return>

c. Restart the print scheduler with the following command:

```
/usr/lib/lpsched<return>
```

8.3 GCCS Desktop Printer Concept of Operations

The purpose of this section is to describe the printing capabilities provided by the GCCS Version 2.1 Session Manager (also known as the Desktop). These printing capabilities consist of Network Printing, Remote Printing, and GCCS Development Support.

8.3.1 Network Printing Support. Network Printing Support allows users to send output to printers on their GCCS network regardless of workstation hardware, print server hardware, and printer hardware, within the limitations of the hardware initially identified as supported by the GCCS COE. The following chart describes the combinations of workstation, print server, and printer hardware that are initially supported in the area of networked printing:

CLIENT	PRINT SERVER	PRINTER(S)
SUN Solaris	SUN Solaris	SPARCPrinter II (NEWSPRINT) POSTSCRIPT Non-POSTSCRIPT (HPCL) EPSON Printer
	HP 9.X	POSTSCRIPT Non-POSTSCRIPT (HPCL) EPSON Printer
HP 9.X	SUN Solaris	SPARCPrinter II (NEWSPRINT) POSTSCRIPT Non-POSTSCRIPT (HPCL) EPSON Printer
	HP 9.X	POSTSCRIPT Non-POSTSCRIPT (HPCL) EPSON Printer

Network Printing Support consists of support to the System Administrator for printer installation and management and support to the user for printer selection. System Administrators and users will be provided support for print queue management, and all of these functions will be presented through graphical user interfaces. System Administration printer support will exist as a distinct GCCS application (Printer Administrator) while user print management will be integrated into the GCCS desktop (the User Print Manager function).

8.3.1.1 Printer Administrator. The Printer Administrator function will provide System Administrators the capability to easily manage the functions associated with adding and deleting printers on the GCCS network. Specifically, the following functions will be provided through the printer administrator user interface:

- Install a connected printer on its attached print server.
- Make a newly installed printer visible to all print clients on the network.
- Remove an installed printer from its attached print server and all print clients on the network.

Additional functions provided that relate to the management of printer assets on the GCCS network are:

- Query current available printer list and update the client during system reboot.
- Modify printer characteristics such as description and location.

Queue management functions are similar to functions provided regular users, except that System Administrators are allowed to perform queue management functions across the network and manage jobs that they did not initiate. The queue management tasks supported are:

- Remove any print job from any print queue.
- Move a print job from one print queue to another.
- Start or stop an active print queue.

8.3.1.2 User Print Manager. The User Print Manager enables the user to select the optimal printer for a given print job. The graphical user interface will display a selection list of available printers that includes such details as printer name, print server name, location, description, printer type, and current status. Current status will show how many jobs are currently waiting to be printed on that printer. From this display, the user will select the printer to be used for a given print task. The user will also be enabled to delete jobs that they have initiated from an active print queue.

8.3.2 Remote (Dial-Up) Printing Support. In order to support Army applications that will be reached by modem (through a terminal controller) from remote installations, those applications must be given a method of allowing their output to be directed to a remote printer, either at the dial-up site or potentially at an entirely different remote site. The known constraints on this requirement are that the solution will only be defined for remote print servers that run Windows 3.1 (or potentially Windows NT) or SUN Solaris, and that only character-based applications will be supported remotely.

The solution to this requirement consists of software in three different areas:

a. The particular configuration of the remote print server
b. The software that manages the available printer list based on remote logins and logouts (session control)
c. The software that actually directs the print job to the printer the user selects.

This requirement has one major built-in limitation. The expected maximum throughput is 9600 baud, based on the use of STU-IIIs as modems. This will severely limit the practical size of jobs that can be printed remotely.

8.3.2.1 Remote Print Server Configuration. The remote print server must have the following software, installed in accordance with GCCS installation guidelines: Windows 3.1 (or potentially Windows NT) and Chameleon NFS. Chameleon will allow the remote print server to accept UNIX lpr commands. Only certain types of printers will be supported as remote printers. The following lists the initial configurations supported for remote (dial-up) printer access:

Application Server	Print Server	Printers
SUN Solaris	SUN Solaris	SPARCPrinter II (NEWSPRINT) POSTSCRIPT Non-POSTSCRIPT (HPCL, HPGL) EPSON Printer
SUN Solaris	PC	EPSON Printer

8.3.2.2 Session Control. When a remote user establishes connectivity to the terminal server and logs into an application, the print support software will include the user's local printer on the list of available printers. When the user disconnects from the session, the user's local printer is removed from the available printer list.

8.3.2.3 Remote Print Software. When a remote user is ready to print from an application on the application server, the user will select from the list of available printers (printers on print servers that are concurrently accessing the terminal server). This is likely to be, but does not have to be, the remote printer at the dial-up users site. The application will send the print command and print file to the associated remote print server for processing.

8.3.3 GCCS Printer Administration User’s Guide. The Network Printer Administration Application will allow System Administrators to install, remove and control access to printers on the GCCS network without requiring them to understand the UNIX print commands. All printer activities revolve around the printer table (Table 8-1), so the GCCS System Administrator should view the network printing status in terms of the contents of the printer table. The following sections are step-by-step instructions for performing the major functions of GCCS network printing.

8.3.3.1 Adding a Printer to a Print Server

a. Set up the printer according to the manufacturer’s instructions. For Newsprint printers, this includes completing the full Newsprint software and hardware installation.
HP printers must be set up to receive serial or parallel input. ASCII and Postscript printers will likely require no special setup.

b. Plug the printer into the appropriate port on the GCCS system that will be the print server. Serial printers require a 2-3 swap (null modem) if connected to a serial port.

c. Run the Printer Admin Tool on the print server system.

d. Select **Option A: "Install a Printer on This Print Server."**

e. Provide a printer name. Names must be 14 characters or less and may not include special characters (dash, underscore, and numerals are allowed).

f. Provide the printer type. Valid GCCS printer types are HPCL, ASCII, Postscript, or Newsprint.

g. Provide the port identification.

h. Provide a printer description. This can be the building, room number, command name, or whatever will help a user identify this printer. Descriptions can be any length, but for the sake of reasonable-looking printer list displays, it is recommended that they be limited to less than 40 characters.

   The Printer Administration software will make the appropriate system calls to install the printer on the server and then will add an entry to printer table for this printer. Printer table entries are of the following format:

   > printer name;host name;printer type;printer description;available on network flag;host O/S;color status

i. If there are no errors reported, the printer can now be used by the host server.

8.3.3.2 Making a Printer Available to the Network

a. Test the printer to ensure that it can be printed to by the host server.

b. Select **Option B: "Make the Print Server Able to Accept Network Print Jobs."**

   The Printer Administration software will make the appropriate system call to make this print server able to accept remote print requests. This option must be run on the host server . This option is only required once for each print server. If an attempt is made to run the option more than once, the software will prompt that there is no need to run this option again.

c. Select **Option C: "Make the Printer Available to Other Network Clients."**

   This option may be run from any system on the network. A list will appear showing printers that have been installed but are not yet available to other systems on the network (i.e., the "available to the network flag" in the printer table is set to "False").

d. Select the printer to be made available to the network.

8.3.3.3 Updating Print Clients on the Network. The Printer Administration software includes a script that runs on system boot-up that brings the system in synchronization with the printer table. Printers that are installed on a client that do not have a corresponding entry in the printer table will be de-installed. Printers that are not installed on the client but exist in the printer table (and have their "available to the network flag" set to "True") are installed. Printers that were not added using the printer administration software will not be affected by this script.

This same script can be run from the Printer Administration main menu by selecting **Option I: "Update Printers on This Print Client."**

8.3.3.4 Removing a Printer from the Network

a. Select **Option E: "Remove a Printer from the Network."**

This option can be run from any system on the network. This option simply sets the "available to the network flag" to "False" for that printer in the Printer Table. All systems that are currently print clients for the selected printer will be de-installed the next time they re-boot or run the "Update Printers on this Print Client" option.

The host server will still be able to print to its attached printer.

8.3.3.5 Removing a Printer from a Server

a. Select **Option F: "De-install a Printer from this Print Server."**

This option must be run on the host server. This option presents a list of printers that are attached to the server on which the site is running the Printer Administration application.

b. Select the printer to de-install. The Printer Administration software will make the appropriate system calls to de-install the selected printer. It will also remove the printer's entry from the printer table.

Clients of this printer will be updated the next time they re-boot or run the "Update Printers on this Print Client" option.

8.3.4 The Current Printer File. Included in the GCCS desktop software is a file that keeps track of the user's current printer. This file is found in the user's home directory and is of the form *.c_p:host_name:session_number* to ensure a unique file name. The current printer file is created each time a user logs into GCCS and remains only as long as the user's current session lasts. During the session, if the user selects a new current printer (using the "File -> Select Printer" option on the GCCS main menu bar) the current printer file will be updated with the new selection.

When a user logs out, two processes occur. First, the contents of the current *.c_p:host_name:session_number* file is copied to a permanent current printer file (called *.c_p* and stored in the user's home directory). Second, the current printer file for that session is deleted.

At login, when the *.c_p:host_name:session_number* file is created, the value in the *.c_p* permanent file (which contains the current printer at the end of this user's last session) is copied into the new current printer file.

If, at login, the *.c_p* file does not contain a currently valid printer (based on the printer table), its value is replaced by the system default printer, which is stored in */h/data/global/EMDATA/config/.c_p:global*.

If no valid printer exists in any of these files, the *.c_p:host_name:session_number* file will contain the literal *NULL*.

8.3.5 The Printer Table. The printer table is the single system reference that maintains the current status for all GCCS printers on the network. It is located in */h/data/global/EMDATA/config/printer_table*.

The printer table contains:

- Printer Entries. Single line entries, one for each current GCCS printer, that describe the printer's installation status to the printer administration software. The format of each printer entry is:

  Name;Host;Type;Description;Available on Network Flag;Host O/S;Color Status

  Name -- printer names are limited by UNIX to 14 characters. Printer names cannot contain special characters (except for '-’, '_', and '.').

  Host -- the system name of the server connected to this printer.

  Type -- GCCS supports four broad classes of printers. The valid GCCS printer types are: Postscript, Newsprint, HPCL, and ASCII. Newsprint printers when they are fully installed will are treated as Postscript.

  Description -- this is a free-text area, limited (for display purposes) to 64 characters. This field can be used to describe the printer's physical location, its capabilities, which organization it belongs to, or any other information that might be helpful to the user.

  Available on the Network -- If this printer is currently available for other clients on the network, this flag should be set to "True." If it is set to "False," only the connected server will be able to print to this printer.

  Host O/S -- The Operating System of the connected server host. Valid options are "HP-UX" and "SunOS."

  Color Status -- This field contains information that is not being used in the initial delivery of GCCS Printer Administration (all printers are set to "B/W"). When color printing is supported by GCCS, this field will be used to direct color output to the correct printers.

Additionally, each printer is associated with a device, although device information is not stored in the printer table. On HP workstations, available devices are Parallel, Serial A, and Serial B. On SUN workstations, a single port represents both the Serial A and Serial B devices (which one is determined by a switch on the device driver itself).

- Blank Lines. As needed for readability.

- Comment Lines. As needed for readability. Comment lines are lines in the printer table that contain the pound character ('#') anywhere in the line.

Blank lines and comment lines in the printer table are ignored by the Printer Administration software.

One note about editing the printer table -- the addition of a new entry or the modification of a current entry results in the affected entry becoming the last line of the printer table.

8.4 Configuring a System to Print Remotely.

This section discusses how to configure a print client under Solaris and HP-UX operating systems.

8.4.1 Configuring Solaris. (The following can also be done using the Printer Administrator tool.)

a. Log on to the print client as **root**.

b. Enter the following command:

```
# lpsystem -t s5 {PRINTSERVER}<return>
```

where PRINTSERVER is the name of the print server

This response will appear:

```
{PRINTSERVER} has been added.
```

Enter the following command:

```
# lpadmin -p {LOCALNAME}  -s {PRINTSERVER} !{PRINTERNAME} <return>
```

where LOCALNAME is the name the printer will be called by the system.
PRINTSERVER is the host name of the print server.
PRINTERNAME is the name of the printer on the remote print server.

If this will be the default printer, execute the following statement:

```
# lpadmin -d {LOCALNAME}<return>
```

```
# accept {LOCALNAME}<return>
```

where LOCALNAME is the name the printer will be called by the system.

```
# enable {LOCALNAME}<return>
```

where LOCALNAME is the name the printer will be called by the system.

c. Check for errors by entering the command:

```
# /bin/lpstat -t<return>
```

8.4.2 Configuring HP-UX

a. Log on to the print client as **root**.

b. Enter the following commands:

```
# /usr/lib/lpshut<return>

# /usr/lib/lpadmin -p{LOCALNAME} -m{PRINTMODEL} /
  -v/dev/null -o{PRINTSERVER} -o{PRINTERNAME} -ob3 <return>
```

where LOCALNAME is the name the printer will be called by the system.
PRINTMODEL is the type of printer.
PRINTSERVER is the host name of the print server.
PRINTERNAME is the name of the printer on the remote print server.

```
# /usr/lib/accept {LOCALNAME}<return>
```

where LOCALNAME is the name the printer will be called by the system.

```
# /usr/lib/enable {LOCALNAME}<return>
```

where LOCALNAME is the name the printer will be called by the system.

```
# /usr/lib/enable {LOCALNAME}<return>
```

where LOCALNAME is the name the printer will be called by the system.

```
# /usr/lib/lpsched<return>
```

SECTION 9. USER ACCOUNT ADMINISTRATION

9.1 Creating and Dropping ORACLE User Accounts

To create and drop user accounts for the ORACLE database, the following procedures are available. They must be run as "root."

If there are problems running these scripts, the System Administrator should first ensure that the file permissions are set correctly. For the files described below, the group should be *dba* and the files should have execute permission for the owner and group. The owner will be *oracle* or *root*. That is, the following UNIX commands may need to be invoked:

```
chgrp dba file_name    # change file's group to 'dba'
chmod 754 file_name    # change permissions so the owner and group can execute the file.
```

Files that exist for creating and dropping ORACLE user accounts are located in */h/COTS/RDBMS/* scripts; they are:

```
create_user.csh
create_user.sql
drop_user.csh
drop_user.sql
```

Of this list, the following scripts can be executed by *root*:

a. **create_user.csh -** This C-shell script can be invoked by *root* to create a GCCS ORACLE user with the default tablespace "USERS," temporary tablespace "TEMP," the default profile, and "CONNECT" privileges. The user will be able to create tables in the default tablespace USERS. (The "CONNECT" privilege allows one to execute ORACLE.) The System Administrator must provide the previously-created UNIX user account name, e.g.:

   ```
   /h/COTS/RDBMS/scripts/create_user.csh gccs_user_name<return>
   ```

b. **drop_user.csh -** this C-shell script is invoked by *root* to drop ORACLE user accounts:

   ```
   /h/COTS/RDBMS/scripts/drop_user.csh gccs_user_name
   ```

If it becomes necessary to grant additional role(s) to a user, as *root*, create the following two scripts in the */h/COTS/RDBMS/scripts* directory:

`grant_role.csh` which is very similar to *create_user.csh*:

```
# !/bin/csh
su - oradba -c "sqlplus -silent / @/h/COTS/RDBMS/scripts/grant_role $1 $2"
exit 0
```

`grant_role.sql` which is somewhat similar to *create_user.sql*:

```
grant &2 to &1;
exit
```

And execute as *root*:

```
      /h/COTS/RDBMS/scripts/grant_role.csh gccs_user_name added_role
```

9.2 Adding User Accounts to GCCS

It is recommended that user accounts be established after all software is loaded on all platforms and NIS+ is initialized.

Two administrative accounts are delivered with the software:
secman - used to add user accounts or profiles.
sysadmin - used to perform system administrator functions, such as installation of new segments.

The installation team will assist the Site Administrator in creating an account for the System Administrator (to be used for user account maintenance) and a basic user account. The following steps must be followed.

9.2.1 Creating User Accounts (Performed at the EM Server's Console.)

a. Log in as **secman**, with proper password.

b. Select **Prefs** from the menu bar. Select **Change Profile** from the menu. Click the **Next** or **Prev** buttons until **SYSADMIN** is displayed in the **Position:** field. Click the **OK** button.

c. Double click the **Security** icon. The **run_security** window displays. Enter the secman's password at the Password: prompt. The **Security Manager** window appears.

d. Select **File** from the menu bar. Select **Create Account** from the menu. The **SECURITY MANAGER: Create Accounts** window appears.

e. Enter the **USER ID:** (8 characters or less).

f. Enter the **USER NAME:** (essentially an administrative comment field. Recommended: section, POC Information including location and telephone #.

Example: ccj6-doc MAJ John Doe 8-6580).

NOTE: Do not use commas or other special characters. Use only letters and numerals.

g. The **USER #** field is filled in by the utility. (This is the UID and it is the last used value plus 1. This number may be edited to re-use old UID #s that have been deleted).

h. Enter the **PASSWORD:** (This will be the user's login password).

i. Enter the **SYBASE SYS ADMIN USERNAME:** (sa).

j. Enter the **SYBASE SYS ADMIN PASSWORD:** (as assigned in Section 5.4).

k. Click the button for the **DEFAULT GROUP:** field. Select from: **admin** (for an administrator account) or **gccs** (for a user account). Click the **Apply** button.

l. Click the button for the **OPTIONAL GROUP:** field. Select from: **admin** (for an administrator account) or **gccs** (for a user account). Click the **Apply** button.

m. Click the button for the **Acct_groups** field. Select from: **root**, **Security Admin**, **System Admin**, or **GCCS Operator** (for a user account). Click the **Apply** button.

n. Click the button **Role** field. Select from: **SSO Default** (user account management and security), **SA Default** (system administration, which is primarily used for installing new software segments), or **GCCS Default** (for a user account). Click the **Apply** button.

o. When all fields are successfully completed, click the **OK** button on the SECURITY MANAGER: Create Accounts window.

p. Select **File** from the menu bar. Select **Exit** from the menu. Click **OK** to the Exit question.

9.2.2 Customizing Profiles. After the System Administrator has registered the new user, a user profile must be assigned for the user.

a. Log in as **secman**, with proper password.

b. Select **Prefs** from the menu bar. Select **Change Profile** from the menu. Click the **Next** or **Prev** buttons until SYSADMIN is displayed in the Position: field. Click the **OK** button.

c. Double click the **Profile** icon. The Profile Manager window appears.

d. Select **File** from the menu bar. Select **Add New User Profile** from the menu. The PROFILE MANAGER: Add New User Profile window appears.

e. Click the button for the **User ID:** field. Select appropriate user from the registered users display.

f. Click the button for the **Project:** field. Select appropriate project from the display.

g. Click the button for the **Position:** field. Select from: GCCSUSER or SYSADMIN in the position display. (This selection is tied to the user's launch window icon selections.)

NOTE: These first three fields of the window are mandatory for user profile creation. The others deal with the organizational structure of the site. They include Directorate, Division, Branch, Section, and Cell.

h. Click on the **OK** or **Apply** button. Select **File** from the menu bar and **Exit** from the menu.

SECTION 10. SOFTWARE LICENSE ADMINISTRATION

10.1 Applix License Setup Procedures

To use Applix the license must be installed. Execute the following to obtain your License Key:

a. Log in as *`root`*

NOTE: The system will identify the site's License Key. Contact the GCCS Hotline at (703) 735-8681 or DSN 653-8681 and provide the License Key and POC (NAME, TEL,FAX). DISA will notify Applix, obtain the licensing information for the site, and FAX it to the site POC, usually within 24 hours.

b. Execute the following:

```
# cd /COTS/APPLIX/axdata <return>
```

c. Two license files will appear: *axlicensedemo, alxicensdat*

1. The following is an example of the information that will be executed when *axlicensedemo* is opened:

```
FEATURE *wgm none 3.000 1-dec-95 0 8B4C1F6D076650F27859 "" DEMO
FEATURE *sps none 3.000 1-dec-95 0 4B7C4F4D381F2609F469 "" DEMO
FEATURE *mbx none 3.000 1-dec-95 0 7BDC2F3D48AF4E68BAB1 "" DEMO
FEATURE *fwp none 3.000 1-dec-95 0 5B4C3FCD88E32B76C59F "" DEMO
FEATURE *fpp none 3.000 1-dec-95 0 4B7C4FED95F02D79C59F "" DEMO
FEATURE *fgp none 3.000 1-dec-95 0 8B4C1FCD58B34B66C59F "" DEMO
FEATURE *dat none 3.000 1-dec-95 0 7BAC2F6D54BF4D6AC7A7 "" DEMO
FEATURE *opn none 3.000 1-dec-95 0 4B7C2FBD8CEBF81AC019 "" DEMO
FEATURE *rts none 3.000 1-dec-95 0 5B3C3F5D2D1027FEF16F "" DEMO
```

2. The following is an example of the information that will be executed when *axlicensdat* is opened:

```
FEATURE *sps none 3.000 1-dec-95 0 4B7C4F4D381F2609F469 "" DEMO
FEATURE *mbx none 3.000 1-dec-95 0 7BDC2F3D48AF4E68BAB1 "" DEMO
FEATURE *fwp none 3.000 1-dec-95 0 5B4C3FCD88E32B76C59F "" DEMO
FEATURE *fpp none 3.000 1-dec-95 0 4B7C4FED95F02D79C59F "" DEMO
FEATURE *fgp none 3.000 1-dec-95 0 8B4C1FCD58B34B66C59F "" DEMO
FEATURE *dat none 3.000 1-dec-95 0 7BAC2F6D54BF4D6AC7A7 "" DEMO
FEATURE *opn none 3.000 1-dec-95 0 4B7C2FBD8CEBF81AC019 "" DEMO
FEATURE *rts none 3.000 1-dec-95 0 5B3C3F5D2D1027FEF16F "" DEMO
```

d. Execute the following:

```
# cd/COTS/APPLIX/
```

e. Type **`applix`**.

f. From the Applix utility menu, select **LICENSEGENERATOR**.

g. Using the license information sheet provided by DISA, enter all information, tabbing between fields. All entries are in upper case.

h. After entering all data, choose **OK**.

NOTE: To purchase Applix license call 1-800-8-Applix or 1-508-870-0300.

i. To ensure that the APPLIX license manager comes up when the system is re-booted, execute the following:

```
# cd  /etc/rc3.d

# vi  S4Sapplix
```

Add the following lines:

```
./h/COTS/APPLIX/axdata/axlnmgrd -c\

./h/COTS/APPLIX/axdata/axlicenseda > /tmp/axnlmlog &
```

10.2 JDISS License Setup Procedures

The JDISS will not run if the site has not obtained a license. Contact the JDISS Hotline at (301-669-5100) to find out how to obtain a license.

10.2.1 Client/Server Relationship. For JDISS to run properly, the JDISS license must be on the host designated "lmserver." The JDISS client segment must be loaded on a host that can reach the lmserver, i.e., the */etc/inet/hosts* file must have the IP address and "lmserver" of the host that has the JDISS server segment loaded.

10.2.2 License File Procedures for JDISS Version 2.0.2.01

NOTE: The license file is called *license.dat* and is in ASCII text format. Most of the file contents should not be changed. The server host ID cannot be changed without getting a new license file from the JDISS PMO. In the DAEMON line, the path to the daemon can be modified. If any other changes are made, it will invalidate the license, and the application will not be found.

If a site has a license, or if the host machine is a client of another host that has a network license:

To install the JDISS license file for JDISS V2.0.2:

a. Copy the *license.dat* file the site received to */h/JDISS/etc* as follows:

```
# cp license.dat /h/JDISS/etc
```

b. Re-boot the machine. Installation is complete.

10.2.3 Procedures for Machines Currently Running JDISS V2.0 or V2.0.1 that Upgrade V2.0.2.

Before upgrading to JDISS V2.0.2, save the *h/JDISS/etc/license.dat* and */h/JDISS/etc/license.dat.2.0.2* files to another directory, so the files will not be deleted.

a. After installing V2.0.2, copy the saved *license.dat.2.0.2* to the JDISS directory as follows:

```
# cp license.dat.2.0.2 /h/JDISS/etc/license.dat
```

NOTE: You are renaming *license.dat.2.0.2* to *license.dat.*

b. Re-boot the machine. Installation is complete.

10.2.4 Procedure For Verifying License Management Server has been Identified

a. Log in as **root**.

b. Execute the following commands:

```
# cd /h/JDISS/Scripts <Return>

# JDISS_startup

# JDISS_boot
```

In both of these files, there is a line that appears as follows:

Replace the "hostname" on the "setenv" line below with the name of the license server "setenv"

```
LM_LICENSE_FILE 7337@hostname
```

where *hostname* represents the name (or alias) of the server that has the license file.

For example:

`setenv LM_LICENSE_FILE 733@ gccshost` ("gccs" is the name of the license server)

c. Save the changes and exit.

NOTE: In JDISS 2.0.1 and JDISS2.0.2, the lmserver will appear as the host name. If that is the case, no changes need to be made. However, *lmserver* must be a valid alias for the machine that is the license server. Try to ping *lmserver*. If unsuccessful, check the */etc/hosts* file and see if the lmserver has been added or changed.

NOTE: In JDISS 2.0, an actual server name was used instead of the lmserver alias. The site may continue to operate with an actual host name specified, but should make sure it is the correct host name! If "uname -n" appears as the host name, the site has a JDISS 2.0 install that never was configured. Change "uname -n" to the actual host name of the license server.

10.2.5 Troubleshooting the JDISS License Installation

10.2.5.1 Problem: The "Pings" Tool Does Not Start. This is a known problem on all GCCS JDISS installations. To fix this problem, execute the following commands, which must be performed as **root**:

```
# ch /h/JDISS/progs <Return>
# chmod 4555 JDISS_pings <Return>
```

10.2.5.2 Problem: The "Pings" Tool Does Not Work. The following error message appears:

```
checkout: pings: cannot find SERVER hostname in network database
```

This problem is known to occur on hosts that are running JDISS as a client. That is, the license file/manager resides on another host (license server). To fix this problem, execute the following commands, which must be performed as **root**:

```
# cd /h/JDISS/data/IXI/Icons/Pings.obj <Return>
# vi activate <Return>
```

Then remove both of the following lines:

```
LM_LICENSE_FILE=/h/JDISS/etc/license.dat
declare exported LM_LICENSE_FILE
```

Save the changes and exit.

10.2.5.3 Problem: The "Chatter" Tool Will Not Start. This is a known problem on all GCCS JDISS installations. A fix has been identified and will be available soon.

10.2.5.4 Problem: The "System Load" Tool Will Not Start. This is a known problem on all GCCS JDISS installations. To fix this problem, execute the following commands as **root**:

```
# cd /h/JDISS/progs <Return>
# chgrp sys JDISS_xload <Return>
# chmod 2555 JDISS_xload <Return>
```

10.2.5.5 Problem: The "Host Tool" Will Not Allow a Save. This problem has been reported on some GCCS JDISS installations. To fix this problem, execute the following commands as **root**:

```
# ch /h/JDISS/etc <Return>
# chmode 666 jdhosts <Return>
```

Re-boot the machine for all of the changes to take effect.

10.3 NeWSprint License Setup Procedures

10.3.1 NeWSprint Version 2.0 Setup Procedure. To install the font license, the site must have a font password. Also, if the site has a Postscript printer, such as a Laserwriter, it does not need a font license.

10.3.1.1 Acquiring a Font Password. A font password can be acquired by calling 1-800-USA-4SUN and supplying the following information.

- Host ID of the system to which the printer is attached.
- Serial number of the NeWSprint software. The serial number is printed around the inside hole of the NeWSprint CD.
- The NeWSprint "right to use" number, listed on the face of the licensing agreement.

After aquiring the password, install the software, and set up the license that was provided by SUN Systems.

10.3.2 Upgrading a License for NeWSprint V2.0 to V.2.1. If a site is using NeWSprint 2.0, the original password is still valid for NeWSprint 2.1. To check the fonts, execute the following:

```
# cd /var/spool/license/fontlicense
```

Example (a number should appear that is similar to this font license: .65000934):

```
# cat /var/spool/licenses/fontlicenses.65000943
```

NOTE: Host ID and font password will be displayed.

NOTE: The installing license procedures are the same as in Section 2.0, "Setup Procedures."

10.3.3 NeWSprint Version 2.5 License Setup Procedures

a. Call SUN Systems at 1-800-USA-4SUN during the hours of 0800 to 1700 Monday through Friday to obtain font password. You must have the same information as listed in Section 2.0.

b. To view the host ID and font password, execute the following:

```
# /opt/NeWSprint/bin/hostid
```

SECTION 12. SECURITY ADMINISTRATION

NOTE: This procedure should be performed last.

After loading the Basic Security Module (BSM) segment, everything will be in place to initiate security auditing. Team GCCS strongly recommends reading Chapter 3 of the *Solaris SHIELD Basic Security Module Manual* prior to installing the BSM segment.

NOTE: At this writing, the BSM segment creates audit files in the /*h*/*data*/*global* area of the filesystem, but there is not sufficient space in this location for large audit files. The GCCS Engineering Office has initiated a change request to create these files in another location. Therefore, a procedure is provided in 12.5 that will move the audit files in the event a new BSM segment is not ready prior to GCCS Version 2.1 fielding.

12.1 Updating from GCCS Version 2.0 to Version 2.1

If a site's system has been upgraded from an existing GCCS Version 2.0 to GCCS Version 2.1, then the SA has already performed the file system configuration tasks to create the security mount points. If in doubt, review the results of the following command:

```
# df - k <Return>
```

Something like the following will be displayed, on a database server:

NOTE: Filesystem names and sizes in this table are for demonstration purposes only, no correlation between this table and an operational GCCS Version 2.1 is intended.

```
Filesystem                     kbytes      used      avail   capacity  Mounted on
/dev/vx/dsk/rootvol             96023     19825      66598      23%    /
/dev/vx/dsk/usr                295382    169295      96557      64%    /usr
/proc                               0         0          0       0%    /proc
fd                                  0         0          0       0%    /dev/fd
/dev/dsk/c0t1d0s0              489702     33029     407703       7%    /var
swap                          1793612        44    1793568       0%    /tmp
/dev/dsk/c1t1d0s0             1952573   1033145     724178      59%    /h1
/dev/dsk/c1t3d0s0             1759749   1179103     404676      74%    /home2
/dev/dsk/c4t2d0s0             1952573  11757322   11757322       0%    /oracle/smback
/dev/dsk/c1t0d0s0             1759749    161841    1421938      10%    /opt
/dev/dsk/c4t3d0s3             1856746    174561    1531838      10%    /security1
/dev/dsk/c4t3d0s0             1856746    174561    1531838      10%    /security2
/dev/vx/dsk/oracledg/vol10    8648108    921396    1861902      90%    /h
/dev/vx/dsk/oracledg/vol01    9218465    275878   16020747       7%    /home10
/dev/dsk/c2t0d0s0             1952573    444059    1313264      25%    /h/USERS
```

```
Filesystem                kbytes    used     avail    capacity  Mounted on
dbserver:/h/data/global   385351    291707   55114      84%     /h/data/global
```

On one of the application servers, the result of the "df" command will look something like the following:

```
Filesystem              kbytes    used     avail     capacity  Mounted on
/dev/dsk/c0t3d0s0       76767     32378    36719       47%     /
/dev/dsk/c0t3d0s6       225247   165188    37539       81%     /usr
/proc                        0        0        0        0%     /proc
fd                           0        0        0        0%     /dev/fd
swap                    489788     4036   485752        1%     /tmp
/dev/dsk/c0t3d0s7       385351   292142    54679       84%     /h
/dev/dsk/c0t1d0s0       819718   455442   282306       62%     /home1
/dev/dsk/c0t0d0s0       1733085  498054   1061731      32%     /home2
/dev/dsk/c0t3d0s5       81807     45051    28576       61%     /opt
/dev/dsk/c0t3d0s3       1007          9      898        1%     /security1
/dev/dsk/c0t3d0s4       1511          9     1352        1%     /security2
mailhost:/var/mail      489702    38589   402143        9%     /var/mail
dbserver:/h/USERS       1952573  480171   1277152      27%     /h/USERS
zeppo:/world            8648108  7688692   94606       99%     /world
```

Notice that on the database server the "security" filesystems are rather large. This is the actual location of the audit files. On an application server (SPARCStation 10/20/5/2) these filesystems will be approximately 1 megabyte in size and act as the mount points for the security auditing file space shared from the database server. If the mount points have not yet been created, refer to the *GCCS Implementation Procedures* to create these mount points.

When a database server is being built, the security partitions will be created during the initial stages of the kernel build. See the disk partitioning schemes in the *GCCS Implementation Procedures* for more information. The following *Korn Shell* script is the portion of the GCCS kernel that creates the shared filesystems for security auditing:

```
# If /security1 or /security2 exists and are mounted file systems they
# will be exported making this system a security audit server.
# If /security1 or /security 2 do not exist entries will be entered
# in the /etc/vfstab file to mount the dbserver /security1 and
# /security2 partitions.

      if [[ -d /security1 || -d /security2 ]]; then
         df -k | grep /security1 > /dev/null 2>&1
            if [[ $? -eq 0 ]]; then
               echo "/security1 exists as a file system, sharing it"
               echo share -F nfs /security1 >> /etc/dfs/dfstab
            fi
         df -k | grep /security2 > /dev/null 2>& 1
            if [[ $? -eq 0 ]]; then
               echo "/security2 exists as a file system, sharing it"
```

```
                echo share -F nfs /security2 >> /etc/dfs/dfstab
             fi
      else
      echo "/security1 and /security2 do not exist on this system"
      echo "placing entries in the /etc/vfstab file to mount the"
      echo "dbserver's /security1 and /security2 partitions"
      mkdir /security1 /security2
echo dbserver:/security1 - /security1 nfs - yes rw,bg,soft >> /etc/vfstab
echo dbserver:/security2 - /security2 nfs - yes rw,bg,soft >> /etc/vfstab

# Modify /sec1 and /sec2 entries in /etc/vfstab to /security1 and /security2
cp /etc/vfstab /tmp/vfstab
sed -e "s/sec1/security1/;s/sec2/security2/" /tmp/vfstab > /etc/vfstab
```

12.2 Initiating the BSM

Prior to starting the Basic Security Module, the audit file directories need to be created:

```
# mkdir /security1/security1/files <return>
# mkdir /security2/security2/files <return>
```

Ensure these directories have the proper permissions and ownership:

```
# cd/security1/security1 <return>
# chgrp staff files <return>
# chmod 2750 files <return>
# cd ../security2/security2 <return>
# chgrp staff files <return>
# chmod 2750 files <return>
```

Once the system has been prepared to accept auditing logs, the BSM segment can be installed like any other segment. Refer to Section 3 of this Manual for more information on using the Segment Installer.

After the BSM segment has been installed, the *Solaris SHIELD Basic Security Module* will need to be activated. Perform the following procedure to do this. This procedure will enable the Basic Security Module in accordance with the default values established by the BSM segment. These values can be altered by skipping this section and editing files described in Section 12.3.

a. Bring system down to single-user mode.

```
#    /etc/telinit 1<return>
```

You will be asked to provide the *root* password to complete the transition to single-user mode.

b. Once the host is in single-user mode, perform the following as **root**.

```
#    cd /etc/security<return>
#    ./bsmconv<return>
```

NOTE: You will have to respond **yes** to a question during this process.

c. Once the *Solaris Shield Basic Security Module* has completed its initialization, you will need to reboot for the auditing to begin.

```
# /etc/telinit 6 <return>
```

d. After the reboot has completed, log in as **root** and check the audit file / *security1*/*files* to see if the login was recorded. If the root login was not recorded, there may be a problem with the permissions on the audit files. The proper permissions for the audit file can be set by performing the following:

```
# cd /security1/security1<return>
# chgrp staff files<return>
# chmod 2750 files <return>
# cd ../security2/security2 <return>
# chgrp staff files <return>
# chmod 2750 files <return>
```

If these permissions are correct, check the status of the audit daemon, *auditd*, by performing the following command:

```
# ps -aef | grep auditd<return>
```

If the audit daemon is running, the previous command should return two lines, one of which will be similar to the following:

```
root 1143    1  80 19:25:03 ?  0:14 /usr/sbin/auditd
```

If the audit deamon is not running, the previous command will return only the presence of the *grep* for the audit daemon. The following is a typical response:

```
root  16453  16446  6  19:25:03  pts/5  0:00 grep auditd
```

If the audit daemon is running and the permissions are correct on the files, any number of possible configuration errors may have occurred. Pages 30 - 35 in the *Solaris SHIELD Basic Security Module* offer good insight to finding what might be wrong. Remember, on-line help is available by referencing the manual pages, e.g., man *auditd*, man *bsmconv*, etc.

12.3 Customizing Auditing

Auditing can be controlled by customizing several files found under / *etc*/*security*. The two files that are most important are *audit_control* and *audit_user*.

The *audit_control* file on each machine is read by the audit daemon at start-up (greater detail on this file is contained on pages 11 through 12 of the *Solaris SHIELD Basic Security Module [SSBSM] Manual*). This file sets the type of auditing desired and the location of the audit files. The *audit_control* file that is created during installation of the BSM segment appears below:

```
dir:etc/security/audit/localhost/files
dir:/var/audit
flags:lo,pe,-fc,-fd,-pr,-fw
minfree:20
naflags:lo,nt
```

The lines that begin with "dir" specify the location of the physical audit files. The field definitions for the other lines (flags, minfree, and naflags) can be found on pages 8 through 11 of the *SSBSM Manual*.

The *audit_user* file is useful if auditing specific users is desired; pages 13 through 14 of the *SSBSM Manual* provide greater detail. The *audit_user* file consists of three fields. The first field is the user name, the second field is the "always audit" field, and the third field is the "never audit" field.

NOTE: If the value of "all" is set in the third (never audit) field then that user will never have any auditing performed.

A sample *audit_user* file appears below:

```
root:lo:no
audit:no:all
```

NOTE: As can be seen in this example, the user named "audit" does indeed have the value of "all" in the third (never audit) field. This shows a case where a user named "audit" has been created, who can log in and perform a set of tasks without being audited. This is sometimes done to avoid the possibility of having to work around the full audit logs, which might result in a locked system.

If such a user is desired, perform the following procedure. (For more information see the *SSBSM Manual*, pages 35 and 36.)

a. # **vi /etc/passwd**<return>

   Add the following entry to the / *etc*/*passwd* file.

   ```
   audit:x:0:1::/:/sbin/sh
   ```

b. # **vi /etc/shadow** <return>

   Add the following entry to the / *etc*/*shadow* file.

   ```
   audit ::::::::
   ```

c. Save both of these files and set the password on audit with the following command:

```
#  passwd audit  {Type in password for audit} <return>
 new passwd:  {Type in password for audit}<return>
```

12.4 Disabling Basic Security Module

This procedure can be run to disable security auditing. A site may need to do this if the system begins to display unwanted behaviors such as panic crashes or random lock-ups. These symptoms have been seen in the past when auditing became excessive. Part of the solution for this unstable behavior is the installation of a set of patches that are loaded during the initial system setup. If for some reason your system becomes unusable, perform the following procedure to disable the Basic Security Module.

a. Put the system in single-user mode by typing:

```
#  su - root<return>
#  cd /<return>
#  sync;sync;init 0<return>
```

If the command line cannot be reached, and log in from another host is impossible, execute the following:

NOTE: This procedure could cause problems with the ORACLE database.

Press the **STOP** and **A** key simultaneously. This will bring the system to the `eeprom` or `OK` prompt line. Then proceed as shown below.

When the system is halted, enter:

```
#  boot -s<return>
#  cd /etc/security<return>
#  ./bsmunconv<return>
```

The following is displayed:

```
Shall we continue the reversion to a non-BSM system? [y/n]

# y <return>

mv: cannot access /etc/security/audit_startup
./bsmunconv:  INFO: The Basic Security Module has been disabled.
Please, reboot your system
```

b. Re-boot the system when *./bsmunconv* is done:

```
#  boot -r <return>
```

12.5 Customizing the Audit File Locations

As stated earlier in this section, the BSM segment might configure audit files in the / *h*/*data*/*global* area of the file system. It is more desirable to place these large files in a part of the file system that has more space dedicated for the purpose of holding audit files. The following changes need to be implemented prior to starting BSM.

- The *audit_control* file will need to be edited to reflect the new location of the audit files.
- The BSM "*audit_download*" script will need to be instructed where to find the audit files to automate the reduction of the audit files for archiving.
- The audit daemon will need to be instructed to re-read the *audit_control* file.

Perform the following procedure to re-direct the location for audit file writing.

a. `# vi /etc/security/audit_control`<return>

b. Change the lines that start with "dir" to read as follows:

From:

```
dir:etc/security/audit/localhost/files
dir:/var/audit
flags:lo,pe,-fc,-fd,-pr,-fw
minfree:20
naflags:lo,nt
```

To:

```
dir:/security1/security1/files
dir:/security2/security2/files
flags:lo,pe,-fc,-fd,-pr,-fw
minfree:20
naflags:lo,nt
```

c. Save this file.

d. Change the value of the variable *log_path*:

From: **`log_path = /h/EM/auditlogs/all_hosts/files/`**

To: **`log_path = /security2/security2/files/`**

e. Save this file.

f. Instruct the audit daemon to re-read the audit control file with the following command:

`# /usr/sbin/audit -s`<return>

The audit logging should now be going to / *security1*/*security1/files*, and the audit files that have been acted upon by the "*auditreduce*" command should be stored in /security2/ *security2*/*files*. The files in */security2/security2/files* should be archived to tape, or other media, and saved as part of the system backup procedures. These files can then be removed with the following command:

```
# rm /security1/security1/*
```

or

```
# rm /security2/security2/*
```

SECTION 13. JMCIS ADMINISTRATION

13.1 Setting Up the JMCIS Software

To set up the JMCIS software to have one machine act as the JMCIS Track database master, perform the following procedures on all workstations that have the JMCIS segments loaded. The machine that is the JMCIS master will be the workstation that receives all traffic and will distribute the Track database to all of its clients. All JMCIS communications will be controlled through this workstation.

a. As **sysadmin**, change directory to the following directory:

```
# cd /h/data/local/UB/System/Network
```

b. Edit all files that end with *host*:

```
# vi *_host
```

Change the *jots1* to the host name of the workstation that is the JMCIS master (if this machine is a JMCIS Standalone, then the user should use his or her own host name:

1. **cw** (change word)
2. **hostname** (i.e., "romeo")
3. **<ESC>**
4. **:w** (write the file)
5. **:n** (go to the next file)
6. **.** (period, repeats last command which was "cw")
7. **:w**

NOTE: Repeat Steps 5 through 7 until a message "no more files to edit" is received.

8. **:q** (quits the file)

c. Change the *hosts* file in this directory:

vi hosts	
/jots1	(type a "slash", then **jots1**; this will find the string *jots1* in the file)
cw	(change word)
hostname	(enter the JMCIS master host name)
<ESC>	
j	(move to the next line)
cw	(change word)
hostname2	(host name of a JMCIS client workstation)
<ESC>	
:w	(write the file)
j	(move to the next line)
dG	(delete to the end of the file)

:wq! (write and then quit the file)

The file should have at least two uncommented lines that look like the following:

```
hostname 1
hostname2 2
```

The entry with the "1" is always the JMCIS master. The entry with the "2" is the first client. The user may change or append any other entries after the first client with increasing trailing numbers (i.e., "hostname3 3"). This will represent more clients to the JMCIS master.

d. Each client must have the JMCIS global data directory *NFS* mounted from the JMCIS master. Verify that the entry in the /*etc*/*vfstab* contains the correct data directory. /*h*/*data*/*global*/*UB* must be mounted off of the JMCIS master. If the JMCIS master is different from the Executive Manager server, separate entries for /*h*/*data*/*global*/*EMDATA*, /*h*/*data*/*global*/*SYSADM*, and /*h*/*data*/*global*/*UB* must be appended to the /*etc*/*vfstab* file.
If this is the case, the /*etc*/*vfstab* should appear as follows:

```
emserver:/h/data/global/EMDATA  - /h/data/global/EMDATA nfs  - yes rw,bg,soft
emserver:/h/data/global/SysAdm  - /h/data/global/SysAdm nfs  - yes rw,bg,soft
jots1:/h/data/global/UB  - /h/data/global/UB nfs  - yes rw,bg,soft
```

(This applies to any other directories in the /*h*/*data*/*global* directory, such *AMHS, JNAVSV, Printer*).

13.2 Setting the JMCIS WAN DDN Unique Identifier

The JMCIS WAN DDN Unique Identifier (UID) is an important piece of information for Track database control across the SIPRNet. This UID must be unique to the site's JMCIS master. If it is not a unique identifier to distinguish the site's JMCIS master from other JMCIS masters, problems may arise when JMCIS tries to perform Track correlation. The site must get a unique identifier for its system. This must be obtained from the GCCS Hotline or OSF.

To set the JMCIS WAN DDN UID, perform the following instructions:

a. Log in as **sysadmin**.

b. In an xterm, execute the following program:

```
/h/AcctGrps/SysAdm/progs/SASetWanUid
```

c. Enter the appropriate three alphanumeric characters (i.e., the unique identifier). Then click **OK**.

13.3 Setting the JMCIS Host Table

For any JMCIS host to communicate with any other JMCIS host, the JMCIS host table must be set. Each host entered into this table must have an entry in the sites' /*etc*/*hosts* table. At this point, the JMCIS software does not use DNS to resolve host names.

To set the JMCIS host table, perform the following functions.

a. Log in as **sysadmin**.

b. In an xterm, execute the following program:

```
/h/UB/progs/HostTable
```

c. Pull in the */etc/hosts* table:

   With the cursor in the "HostTable" window, push and hold the right mouse button. Select **UPDATE** from this box.

d. Edit each entry and assign a Unique Host ID (UHID) to each host. These UHID's are only applicable to the site's local JMCIS host. The UHID's do not need to correspond to any table and can be assigned arbitrarily.

e. Save this table.

13.4 Setting Up Network Communications

To establish a network channel for the JMCIS software:

a. Log in as a user.

b. From the "Comms" Menu, select **Communications**.

c. In this window, press and hold the right mouse button and then select **Select All**.

d. Press **Delete**. All entries will disappear.

e. Press **Add**. An additional window will appear.

f. In this window, enter in a name for the channel (suggestion: **NETWORK**)

g. Enter a channel XREF (suggestion: **NET**). This XREF must be unique to that channel; i.e., a site cannot add another channel with the same XREF.

h. Scroll through the list at the bottom of the window and highlight the **NETWORK** option.

i. Select **OK**, and the "Communications" window will reappear.

j. Highlight the NETWORK channel just created, and then select **Edit**.

k. On the button bar, press and hold the left mouse button and select the **JMCIS Master** from this list.

l. Click on **AutoStart**. Then select **OK**.

m. Highlight the **NETWORK** option, press and hold the right mouse button and select **Activate** from this window. The network channel should now be active and the site should be able to send and receive messages through this interface.

13.5 Setting Up the MDX Communications

a. From the "Communications" window, select **ADD**.

b. Enter a name for an MDX channel (suggestion: MDX1).

c. Enter an XREF for the MDX channel.

d. Select **MDX** from the scroll list, then select **OK**.

e. From the "Communications" window, highlight the **MDX** entry just created, then select **Edit**.

f. In this window, the user must coordinate the site's entries with the site that will be sending an MDX feed. The user will need to enter the host name that will be sending the data.

SECTION 14. GSORTS ADMINISTRATION

14.1 Downloading GSORTS Database

Unlike any other GCCS application, each site's GSORTS database is initialized and maintained remotely by the Pentagon's JEXACR GSORTS office. Each GCCS site need only request they do so.

The request is made to the GCCS Hotline for JEXACR to put a full, SECRET, GSORTS database at a site. From then on, the JEXACR office will handle all details and ongoing operational support of the GSORTS database, and the site will have the data available for retrieval.

Some services provided by JEXACR are:

a. Initial download of a full GSORTS database to the site's database server.

b. Execution of ORACLE scripts to load the GSORTS database into the GCCS Version 2.1 ORACLE structure, created when GSORTS' segments were installed on the site database server

c. Twice-daily database update service.

To check on the GSORTS database status, a user can either use the GSORTS icon or go to an xterm and use *sqlplus*.

To use the GSORTS icon:

a. Click on the **GSORTS** icon.

b. Select **Options->Database Last Update**

c. Look at the date. If not within the last day or two, then the database is not current. If the date is 19 January 1995 or earlier, it is likely that only the test database is loaded.

To use *sqlplus*:

a. Start an xterm

b. Input the following:

```
# source /opt/bin/coraenv<return>
```

c. Execute the following:

```
# sqlplus /<return>
```

(assumes the user has the GSORTS role)

d. Select **max(bupdate)** from *bide table*.

e. Look at the date. If not within the last day or two, then the database is not current. If the date is 19 January 1995 or earlier, it is likely that only the test database is loaded.

14.2 Using CDROM Maps

GSORTS provides a mechanism to look at Defense Mapping Agency (DMA) Arc Digital Raster Graphic (ADRG) maps. Unlike other applications that require reading the ADRGs from CDROM and downloading to disk, GSORTS will immediately read and display the ADRG CDROM contents. In an operations center, the time (and disk) savings can be substantial.

Unfortunately, within the GCCS environment, and especially with Solaris Version 2.3, many problems at the operating system level conspire to make use of the CDROMs difficult. We do not yet have a formula that will ensure success in using CDROMs with GSORTS within GCCS.

There are several problems with CDROMs, GSORTS, and GCCS:

a. The Solaris Version 2.3 Volume Manager (volmgr) takes over the control of mounting CDROMs.

b. The nearest CDROM drive to a given user may require substantial UNIX-level work to be accessible by GSORTS.

c. Old (pre-1989) ADRG CDROMs will not read correctly.

Addressing each problem in turn:

a. The Solaris Version 2.3 volmgr usually will automount any CDROM put into the disk drive. This means that the user should not use the GSORTS **MapUtilities->AdrgMaps->New CDROM** menu item. Go directly to the **Open CDROM Map** selection. If there is a file name in the list box, then pick the name and everything will work normally. If not, then the troubleshooting process begins. Again, we do not have answers to all situations and cannot re-create all problems. The Solaris Version 2.3 volmgr is not completely characterized. Usually, the user has to do an "eject" command from an xterm.

b. As a first attempt to use CDROM maps, be sure and try a CDROM drive connected physically as part of the SPARCstation 20 application server on which GSORTS is executing. Do not spend time trying to get an xterm SPARCstation 5's CDROM drive to be visible to GSORTS until a CDROM drive on the machine on which the GSORTS software is executing works.

c. If the ADRG CDROM is pre-1989, do not use it. Solaris Version 2.3 volmgr cannot read them.

A hint for troubleshooting:

Try doing operating system commands as **root**. For example, issue the command **eject** (to get the CDROM out). This will bypass permissions problems.

SECTION 15. HARDWARE ADMINISTRATION

15.1 Fiber Distributed Data Interface

Within GCCS, the Fiber Distributed Data Interface (FDDI) will be installed as a selected package (SUWnf) immediately after the core UNIX environment is installed. This package contains the drivers and system changes required to support FDDI. Every SUN SBUS card is currently shipped with a UTP interface installed. To prevent conflicts in the resolution of IP addresses and host names, each enabled network interface must be assigned a unique host name and IP address.

15.1.1 Procedures for Installing FDDI Interface Software.

a. Preparation:

1. Install core UNIX operating systems (recommended patches not as yet installed).

2. Determine FDDI IP address (must be different from ethernet IP address if any).

3. Determine FDDI host name (must be different from ethernet hostname if any).

4. Connect MAC connector from SPARC to FDDI hub.

b. Insert FDDI CDROM in drive.

c. Log in as **root**.

d. To install FDDI patch, execute the following:

```
# /usr/sbin/pkgadd -d /cdrom/fddi_3_0/Solaris_2.x
```

The following will appear on your screen:

```
The following packages are available:
   1 SUWnf FDDI/S Driver/Utilities
          (sparc) 3.0

Select package(s) you wish to process (or "all" to process all
packages). (default: all) [?,??,q]:    1 <Return>
```

e. Specify the nf0 (FDDI) host name. This name must be different from the le0 (ethernet) host name:

```
What host name do you want to use for nf<inst>: <HOSTNAME>
```

f. Specify the nf0 (FDDI) host name. This name must be different from the le0 (ethernet) host name:

```
What ip address do you wish to use for <HOSTNAME>
```

g. Do not specify the SunNet Manager daemons:

```
Do you want to start the SunNet Manager daemons for SunLink FDDI/S
at boot time? [n] [y,n,?,q]   n
```

h. Confirm the installation of files with *setuid*/*setgid* permission:

```
Do you want to install these setuid/setgid files [y,n,?,q]     y
```

i. Confirm the execution of the post-installation script with superuser permission:

```
this package contains scripts which will be executed with
superuser permission during the process of installing the package.

Do you want to continue with the installation [y,n,?]     Y
```

j. Confirm that the installation was successful:

```
Installation of <SUNWnf> was successful.
```

k. Terminate the *pkgadd* program:

```
The following packages are available:
   1 SUWnf FDDI/S Driver/Utilities
          (sparc) 3.0

Select package(s) you wish to process (or "all" to process all
packages). (default: all) [?,??,q]:   q <Return>
```

l. Eject the CDROM:

```
# eject cdrom
```

m. Re-boot the system:

```
# sync;sync;reboot
```

n. Proceed with the installation of additional drivers, packages, or patches.

o. Proceed with the installation of GCCS.

15.1.2 3800 Router Configuration (Example). The following text is provided to illustrate what should appear at the console as the user enters the commands to activate the FDDI interface of the router. This example was produced in the GCCS lab using the Synoptics 3000S Intelligent Hub, in which the router is named 'gccslab' and the configuration was already resident in the router. Text shown in **bold** is what is entered from the keyboard. Additional comments are shown in parentheses.

```
gccslab) en

Password:    (the password will not echo)
gccslab# sh flash
```

```
4096K bytes of Flash address space sized on CPU board.
Memory type is Flash.
File  name/status
 0  xk09190z       (Currently utilized module)
 1  xk91450z       (FDDI module)
 [1499584/4194304 bytes free/total]

gccslab# config t

Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
no boot system flash xk09190z  (disable old flash module)
boot system flash xk91450z  (enable new module)
^Z   (exit configuration mode)

gccslab#
%SYS-5-CONFIG_I: Configured from console by console ()

gccslab# write mem
[OK]
gccslab# exit




gccslab con0 is now available




Press RETURN to get started.
```

15.2 Synoptics 300S Intelligent HUB Introduction

This subsection is provided to assist with the installation of the Synoptics 3000S Intelligent HUB. It provides several types of information:

- The purpose of the HUB - Notes relative to installation.

- Inventory - What and how many of each component to expect.

- Router Configuration - How to activate the FDDI router port.

- Network Management Module (NMM) Configuration - How to perform basic configuration.

In addition to the above information, there are also configuration examples for both the router and the NMM modules.

This subsection is intended as an aid to the installation teams in getting them online to a network that will facilitate server installation. It is not intended to be a complete manual for the Synoptics HUBs.

15.2.1 Purpose of the HUB. The FDDI components are intended solely for the connection of GCCS servers. Each server will be linked to the hub utilizing fiber connections in a single attached mode. It may be necessary to connect the SUN servers to one of the Ethernet boards until the FDDI connection cables are shipped to the site. If this is the case, there will be a 10baseT Ethernet host module provided for this purpose.

The FDDI connections cannot be accomplished at this time because the required cables are not yet available. Separate instructions for making these attachments will be provided when these cables are received.

The router is intended to be utilized to make the bridge between the token-passing protocol of the FDDI components and the CSMA/CD components of the Ethernet side. Although this is the primary purpose of the router, it can be utilized for additional functions if an additional interface is added.

The FDDI-to-router connections will be accomplished via the ports provided in the front of the hub. Patch cables will connect from the router port to one of the FDDI ports. These cables are not yet available but will be shipped with instructions when they are received.

The Ethernet Network Management modules only are provided for this installation. Although two are provided, only one is required and only one should be installed. A separate Ethernet segment may be set up at a later time, or the second module can be kept as a back-up.

The Ethernet components of the hub are intended for connection of either individual GCCS workstations, or LAN segments to which workstations are in turn attached. Ethernet connections can be made to individual workstations on an as-needed basis. The Ethernet host modules supplied should match the network infrastructure at the site.

15.2.2 Inventory. The Intelligent HUB inventory should include the items shown in Table 15-1.

Table 15-1. Synoptics 3000S Hub Components

Synoptics 3000S HUB Components		
Item	**Quantity**	**Comments**
3000S	1	Chassis only.
Power Supply	1	Install in right-most chassis slot.
3904	1 - 3	FDDI Host Module (Quantity varies by site)

Synoptics 3000S HUB Components		
3800	1	Router Card with 1 Ethernet Interface.
3809	1	FDDI Interface for 3800 Router (to be installed on the 3800 router card).
3313A	2	Ethernet Network Management Module. Only one of these cards should be installed with the initial installation.
3301	2	10baseT Ethernet Host Module. Included if site has existing 10baseT infrastructure or if it is required for interim server connections.
* 3304A	2	10baseFL Ethernet Host Module. Included only if site has existing infrastructure that is 10baseFL.
* This item is not included if there is no Ethernet fiber infrastructure at the site.		

A complete set of manuals for the hardware is included in the shipping containers, including a set of router manuals included with the Model 3800 router module. This router module is actually a CISCO Model 4000 router, and configuration is done accordingly.

Subassembly for boards to be inserted into the 3000S chassis is limited to the FDDI Personality module for the router. A complete set of detailed instructions is included with the module. Follow them carefully. If the installer is not comfortable with this type of work, and there is no member of the team who is comfortable doing this assembly, request assistance from the site POC for this equipment.

NOTE: The position of the boards in the chassis is unimportant, except for the power supply, which must be located in the far right position.

15.2.3 Configuration of 3800 Router Module. The router is present in this configuration to perform the translation between the FDDI and the Ethernet sides of the network. This document is not meant to detail how to configure CISCO routers, but is intended to augment a standard configuration that is assumed to be already in place.

In the hardware installation manual for the 3809 FDDI router Personality manual, there is reference to flash modules that must be loaded prior to being able to configure this interface. Specific steps for accomplishing this load are provided in Table 15-2.

Table 15-2. Configuration of 3800 Router

3800 Router Configuration		
#	Command	Description
1	 en	Attach a terminal or a PC to the console port of the 3800 router module. Enter Enable mode. This requires a password.
2	sh flash	Display the file names currently stored in system flash memory. There should be two files shown; make note of both names. The first, (file 0) is the current image and the second, (file 1) is the one that must be used for FDDI.
3	config t	Enter configuration mode from the terminal.
4	no boot system flash xk09190z	Disable the old software module which does not include the FDDI driver. (file 0)
5	boot system flash xk91450z	Specify the proper file for enabling the FDDI interface. (file 1)
6	^z	Exit from configuration mode.
7	write mem	Write the new configuration to system memory.
8	exit	Exit from console. The FDDI interface can now be configured using standard configuration commands.

15.2.4 Configuration of 3313A Ethernet Network Management Module. The NMM for Ethernet can be configured with an IP address, and should be configured if network management is to be performed. The following sequence of steps in Table 15-3 details how to configure the NMM for Ethernet.

Table 15-3. Configuration of 3313A Ethernet NMM

3313A NMM Configuration		
#	Command	Description
1	^C	Connect cable to service port. Typing '^C' brings up the main menu (NOTE: the C is Capital.)
2	m	Toggle boot mode to EEPROM.
3	p	Toggle boot protocol to IP.
4	o	Toggle management protocol to IP.
5	i	Toggle image load mode to local.
6	j	Enter IP configuration menu.
7	a	Set IP address (obtained from site administrator).
8	a	Set default gateway (Same as defaultrouter in most cases).
9	<esc>	Exit back to boot mode menu.
10	w	Write boot config to EEPROM.
11	g	Execute power-up boot sequence; this will re-boot the module and display a banner requesting '^Y' for additional menu.
12	^Y	Enter load menu.
13	i	Enter the protocols parameter menu.
14	i	Enter IP parameters menu.
15	s	Set subnet mask (obtained from site administrator).
16	<look at screen>	Verify the correctness of IP information.
17	<esc><esc>	Return to main menu.
18	w	Write information to EEPROM.
19	z	Reset the 3313A.
20	<fini>	Remove the serial cable.

SECTION 16. CONFIGURING PCs TO DISPLAY DESKTOP

No single PC X-package or TCP has been selected for GCCS. Appendix B contains an evaluation of the leading X and TCP packages.

16.1 X-Package Installation

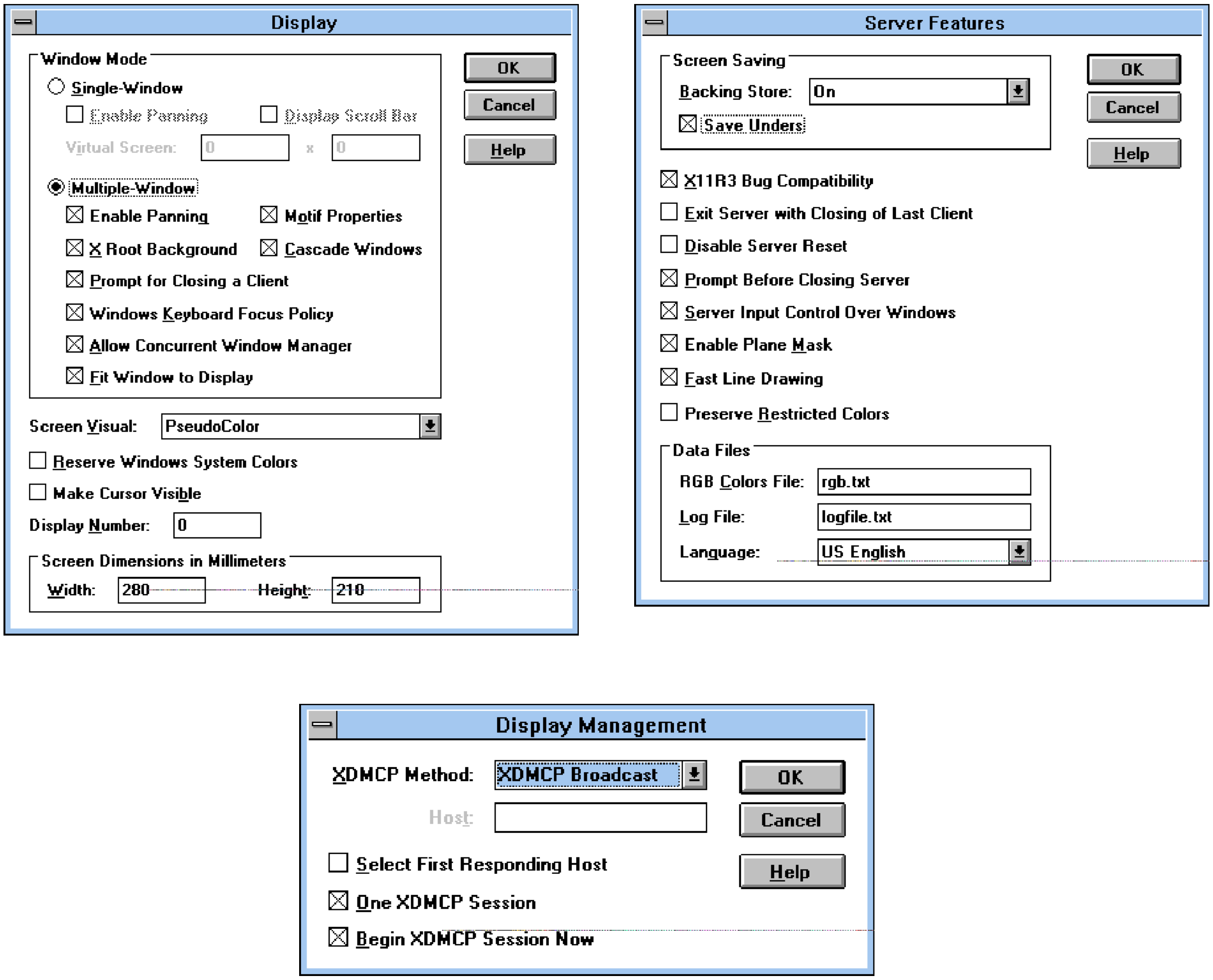
This section contains the screen captures of the options and selection for each of the X-packages evaluated. In all cases the installation selection should be "custom" or "selective" (as opposed to letting the package software automatically do the configuration). This non-automatic installation is required since all fonts must be installed.

16.1.1 Preparation for Installation. Prior to beginning installation, the following information should be gathered:

Software Serial Number (if required by vendor)
Authorization Code (if required by vendor)
Network Software (TCP) Package Used
Network Adapter
Host Name
Host IP Address
Domain Name
IP of Domain Name Server (DNS)
Site Subnetwork

16.1.2 Screen Setups. The following pages show the screen setups for each of the X-packages evaluated.

16.1.3 XoftWare/32. XoftWare/32 has a single menu that appears when its desktop icon is clicked on. The customization of the appearance and operation of XoftWare/32 is via the Options menu. Select **Options** from the main menu to access these features. Figure 16-1 provides screen captures of the options and selections.



Display

Window Mode

○ Single-Window

□ Enable Panning □ Display Scroll Bar

Virtual Screen: 0 x 0

● Multiple-Window

☒ Enable Panning ☒ Motif Properties

☒ X Root Background ☒ Cascade Windows

☒ Prompt for Closing a Client

☒ Windows Keyboard Focus Policy

☒ Allow Concurrent Window Manager

☒ Fit Window to Display

Screen Visual: PseudoColor

□ Reserve Windows System Colors

□ Make Cursor Visible

Display Number: 0

Screen Dimensions in Millimeters

Width: 280 Height: 210

Server Features

Screen Saving

Backing Store: On

☒ Save Unders

☒ X11R3 Bug Compatibility

□ Exit Server with Closing of Last Client

□ Disable Server Reset

☒ Prompt Before Closing Server

☒ Server Input Control Over Windows

☒ Enable Plane Mask

☒ Fast Line Drawing

□ Preserve Restricted Colors

Data Files

RGB Colors File: rgb.txt

Log File: logfile.txt

Language: US English

Display Management

XDMCP Method: XDMCP Broadcast

Host:

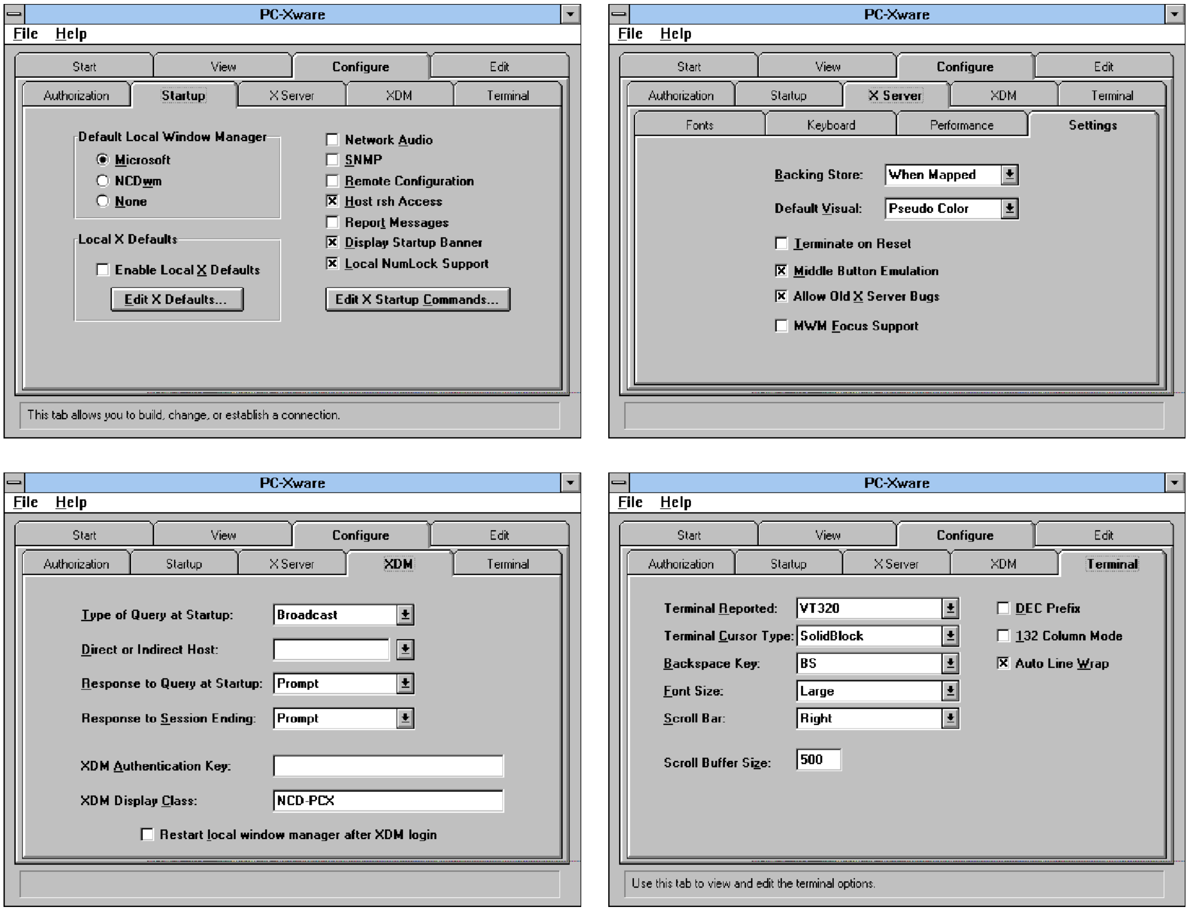
□ Select First Responding Host

☒ One XDMCP Session

☒ Begin XDMCP Session Now

Figure 16-1. XoftWare/32 Screen Captures

16.1.4 PC-Xware. PC-Xware allows customization of features governing the way the X server operates. To configure the PC-Xware configuration options, select the **Configure - Xserver** tab. Figure 16-2 provides screen captures of the options and selections.



Default Local Window Manager
● Microsoft
○ NCDwm
○ None

Local X Defaults
□ Enable Local X Defaults

□ Network Audio
□ SNMP
□ Remote Configuration
☒ Host rsh Access
□ Report Messages
☒ Display Startup Banner
☒ Local NumLock Support

This tab allows you to build, change, or establish a connection.

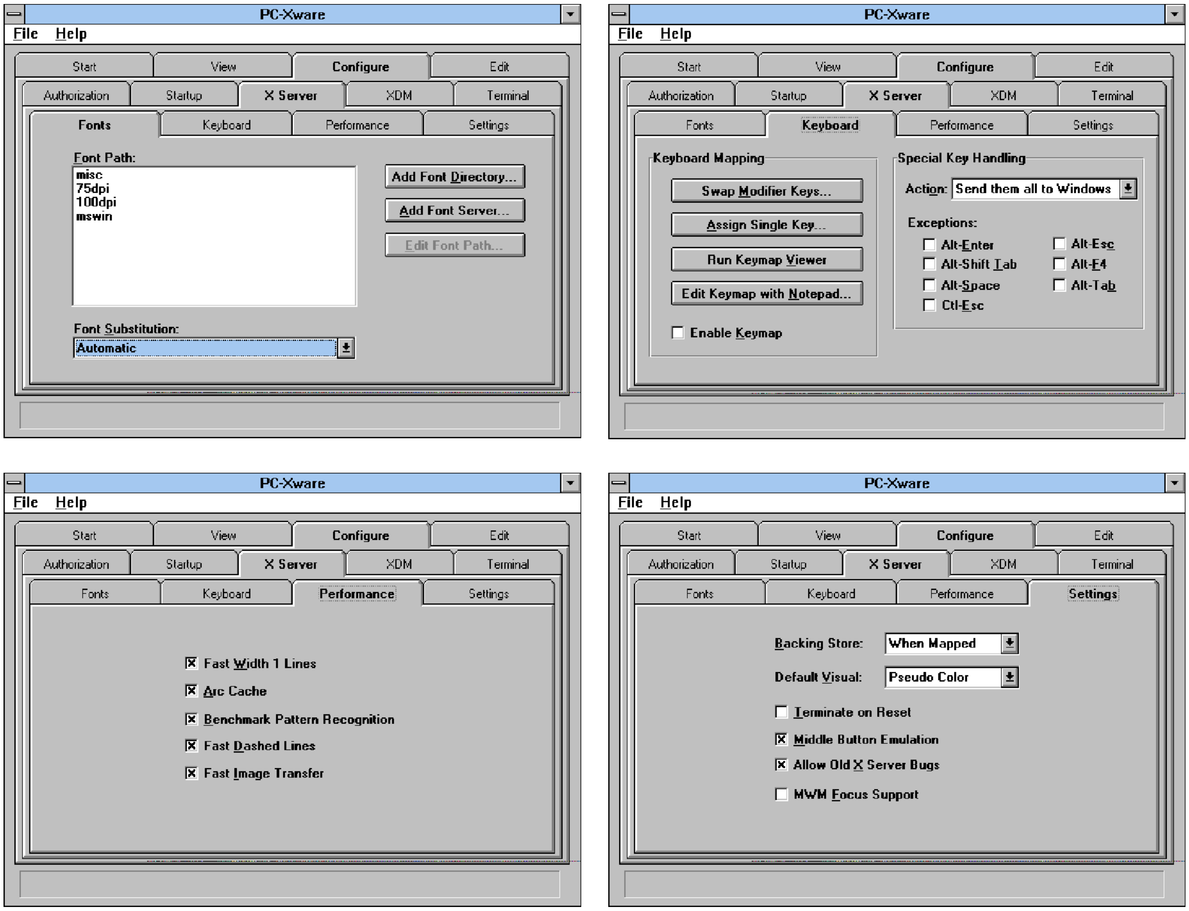
Backing Store: When Mapped
Default Visual: Pseudo Color
□ Terminate on Reset
☒ Middle Button Emulation
☒ Allow Old X Server Bugs
□ MWM Focus Support

Type of Query at Startup: Broadcast
Direct or Indirect Host:
Response to Query at Startup: Prompt
Response to Session Ending: Prompt
XDM Authentication Key:
XDM Display Class: NCD-PCX
□ Restart local window manager after XDM login

Terminal Reported: VT320
Terminal Cursor Type: SolidBlock
Backspace Key: BS
Font Size: Large
Scroll Bar: Right
Scroll Buffer Size: 500
□ DEC Prefix
□ 132 Column Mode
☒ Auto Line Wrap

Use this tab to view and edit the terminal options.

Figure 16-2. PC-Xware Screen Captures (1 of 2)



Font Path:
misc
75dpi
100dpi
mswin

Font Substitution: Automatic

Keyboard Mapping

☐ Enable Keymap

Special Key Handling

Action: Send them all to Windows

Exceptions:

☐ Alt-Enter
☐ Alt-Shift Tab
☐ Alt-Space
☐ Ctl-Esc
☐ Alt-Esc
☐ Alt-F4
☐ Alt-Tab

☒ Fast Width 1 Lines
☒ Arc Cache
☒ Benchmark Pattern Recognition
☒ Fast Dashed Lines
☒ Fast Image Transfer

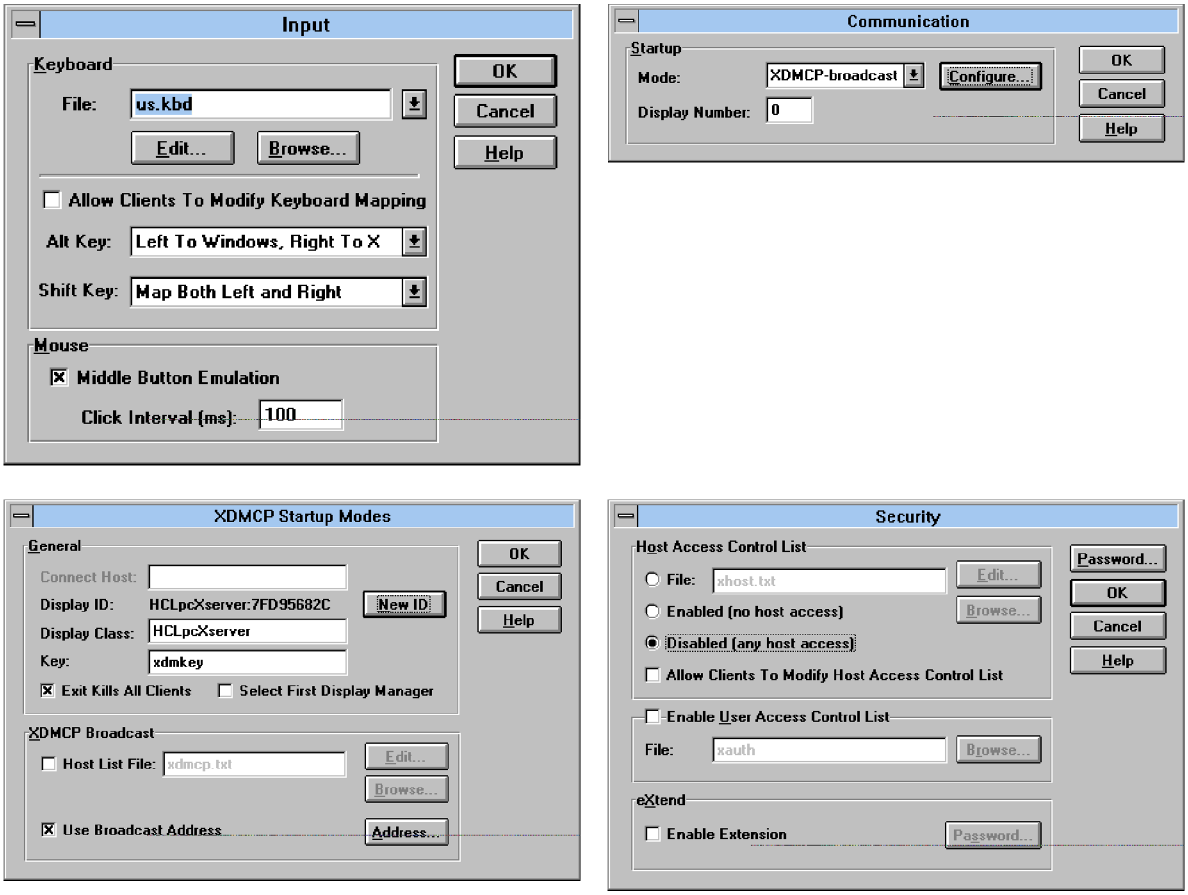
Backing Store: When Mapped

Default Visual: Pseudo Color

☐ Terminate on Reset
☒ Middle Button Emulation
☒ Allow Old X Server Bugs
☐ MWM Focus Support

Figure 16-2. (2 of 2)

16.1.5 eXceed 4 for Windows. To configure eXceed 4 Windows features, start the "Xconfig" program. A dialog box is displayed, displaying icons for each type of setting or function available. Figure 16-3 provides screen captures of the options and selections.



Input

Keyboard

File: us.kbd

Edit... Browse...

□ Allow Clients To Modify Keyboard Mapping

Alt Key: Left To Windows, Right To X

Shift Key: Map Both Left and Right

Mouse

☒ Middle Button Emulation

Click Interval (ms): 100

OK Cancel Help

Communication

Startup

Mode: XDMCP-broadcast Configure...

Display Number: 0

OK Cancel Help

XDMCP Startup Modes

General

Connect Host:

Display ID: HCLpcXserver:7FD95682C New ID

Display Class: HCLpcXserver

Key: xdmkey

☒ Exit Kills All Clients □ Select First Display Manager

XDMCP Broadcast

□ Host List File: xdmcp.txt Edit... Browse...

☒ Use Broadcast Address Address...

OK Cancel Help

Security

Host Access Control List

○ File: xhost.txt Edit... Browse...

○ Enabled (no host access)

● Disabled (any host access)

□ Allow Clients To Modify Host Access Control List

□ Enable User Access Control List

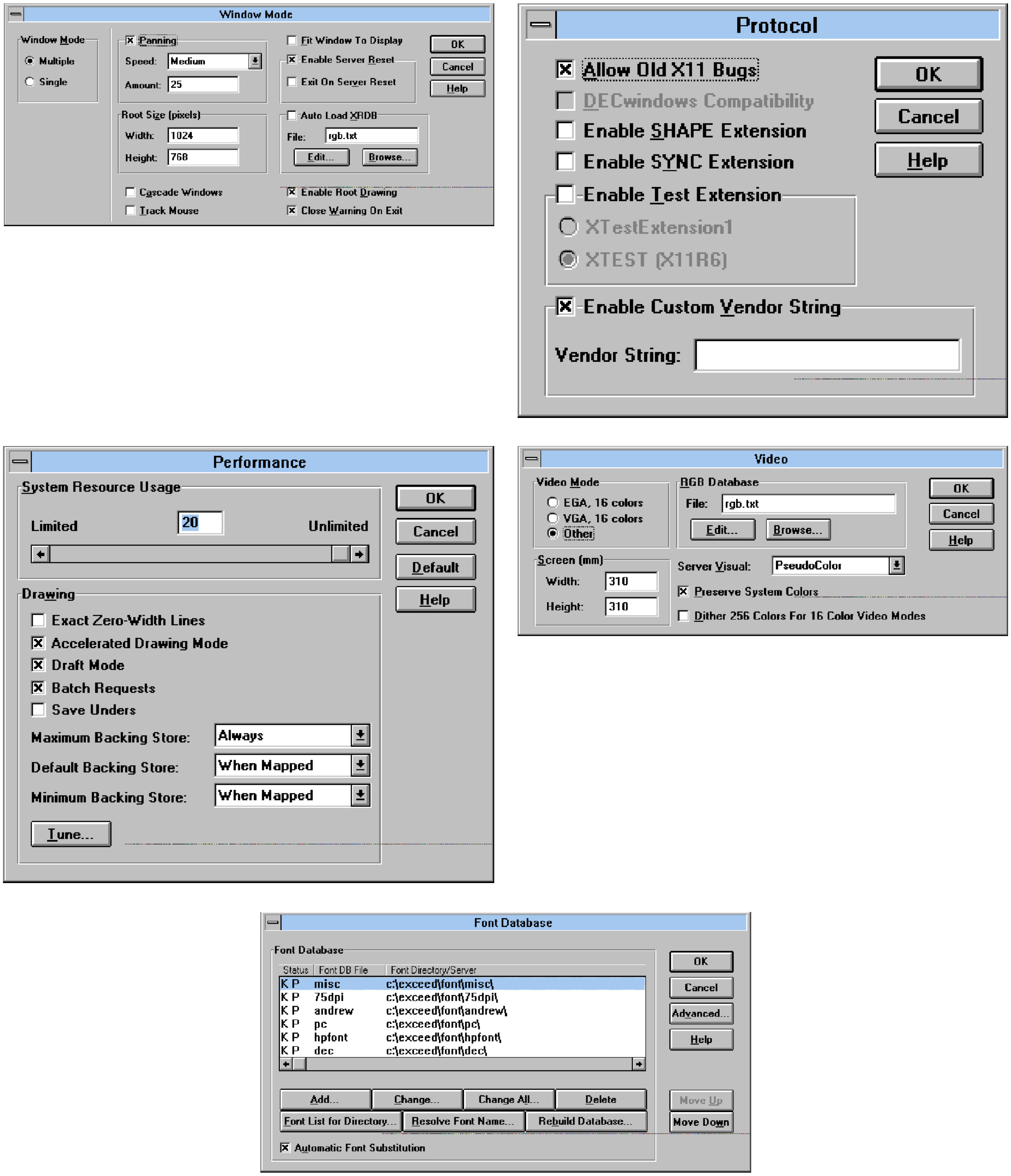
File: xauth Browse...

eXtend

□ Enable Extension Password...

Password... OK Cancel Help

Figure 16-3. eXceed 4 Windows Screen Captures (1 of 2)



Window Mode

Window Mode
- ● Multiple
- ○ Single

☒ Panning
Speed: Medium
Amount: 25

☐ Fit Window To Display
☒ Enable Server Reset
☐ Exit On Server Reset

Root Size (pixels)
Width: 1024
Height: 768

☐ Auto Load XRDB
File: rgb.txt

☐ Cascade Windows
☐ Track Mouse
☒ Enable Root Drawing
☒ Close Warning On Exit

Protocol

☒ Allow Old X11 Bugs
☐ DECwindows Compatibility
☐ Enable SHAPE Extension
☐ Enable SYNC Extension
☐ Enable Test Extension
- ○ XTestExtension1
- ● XTEST (X11R6)

☒ Enable Custom Vendor String
Vendor String:

Performance

System Resource Usage
Limited 20 Unlimited

Drawing
☐ Exact Zero-Width Lines
☒ Accelerated Drawing Mode
☒ Draft Mode
☒ Batch Requests
☐ Save Unders

Maximum Backing Store: Always
Default Backing Store: When Mapped
Minimum Backing Store: When Mapped

Video

Video Mode
- ○ EGA, 16 colors
- ○ VGA, 16 colors
- ● Other

RGB Database
File: rgb.txt

Screen (mm)
Width: 310
Height: 310

Server Visual: PseudoColor
☒ Preserve System Colors
☐ Dither 256 Colors For 16 Color Video Modes

Font Database

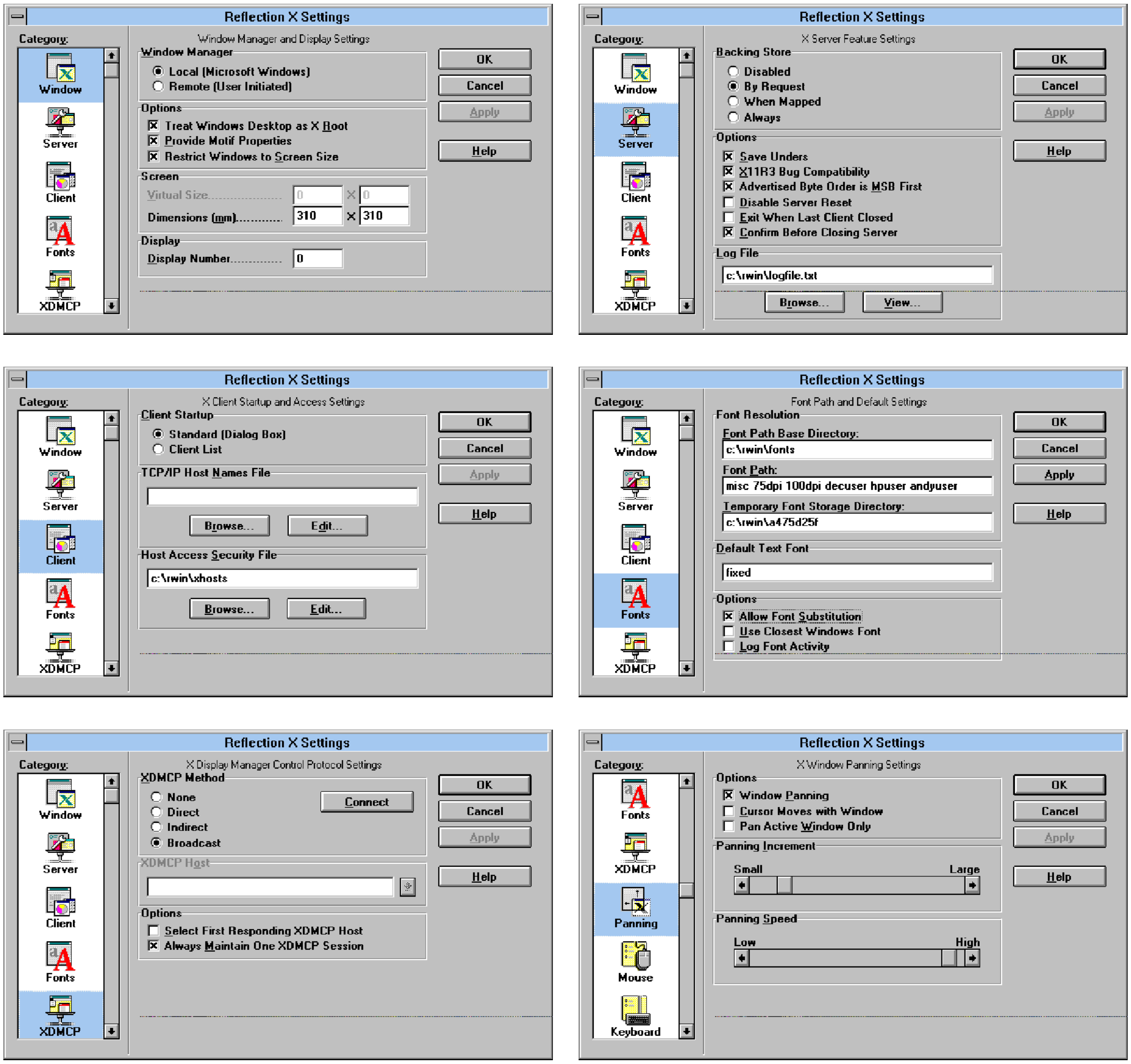
Font Database

Status	Font DB File	Font Directory/Server
K P	misc	c:\exceed\font\misc\
K P	75dpi	c:\exceed\font\75dpi\
K P	andrew	c:\exceed\font\andrew\
K P	pc	c:\exceed\font\pc\
K P	hpfont	c:\exceed\font\hpfont\
K P	dec	c:\exceed\font\dec\

☒ Automatic Font Substitution

Figure 16-3. (2 of 2)

16.1.6 Reflection-X. Reflection-X allows customization of features governing the way the X server operates by selecting the tools option from the desktop icon. Then select the icon of the feature to configure. Figure 16-4 provides screen captures of the options and selections.



Reflection X Settings — Window Manager and Display Settings

Window Manager
● Local (Microsoft Windows)
○ Remote (User Initiated)

Options
☒ Treat Windows Desktop as X Root
☒ Provide Motif Properties
☒ Restrict Windows to Screen Size

Screen
Virtual Size............ 0 × 0
Dimensions (mm)............ 310 × 310

Display
Display Number............ 0

Reflection X Settings — X Server Feature Settings

Backing Store
○ Disabled
● By Request
○ When Mapped
○ Always

Options
☒ Save Unders
☒ X11R3 Bug Compatibility
☒ Advertised Byte Order is MSB First
☐ Disable Server Reset
☐ Exit When Last Client Closed
☒ Confirm Before Closing Server

Log File
c:\rwin\logfile.txt

Reflection X Settings — X Client Startup and Access Settings

Client Startup
● Standard (Dialog Box)
○ Client List

TCP/IP Host Names File

Host Access Security File
c:\rwin\xhosts

Reflection X Settings — Font Path and Default Settings

Font Resolution
Font Path Base Directory:
c:\rwin\fonts
Font Path:
misc 75dpi 100dpi decuser hpuser andyuser
Temporary Font Storage Directory:
c:\rwin\a475d25f

Default Text Font
fixed

Options
☒ Allow Font Substitution
☐ Use Closest Windows Font
☐ Log Font Activity

Reflection X Settings — X Display Manager Control Protocol Settings

XDMCP Method
○ None
○ Direct
○ Indirect
● Broadcast

XDMCP Host

Options
☐ Select First Responding XDMCP Host
☒ Always Maintain One XDMCP Session

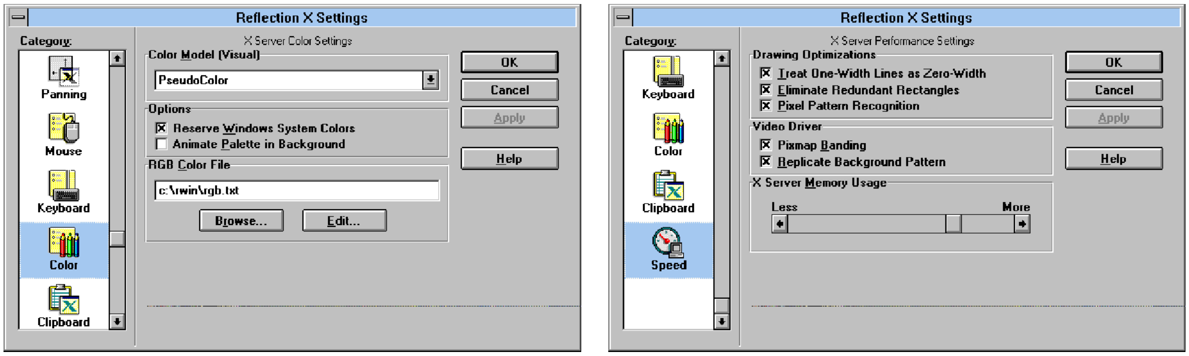
Reflection X Settings — X Window Panning Settings

Options
☒ Window Panning
☐ Cursor Moves with Window
☐ Pan Active Window Only

Panning Increment
Small Large

Panning Speed
Low High

Figure 16-4. Reflection X Screen Captures (1 of 2)



X Server Color Settings

Color Model (Visual): PseudoColor

Options
☒ Reserve Windows System Colors
☐ Animate Palette in Background

RGB Color File: c:\rwin\rgb.txt

X Server Performance Settings

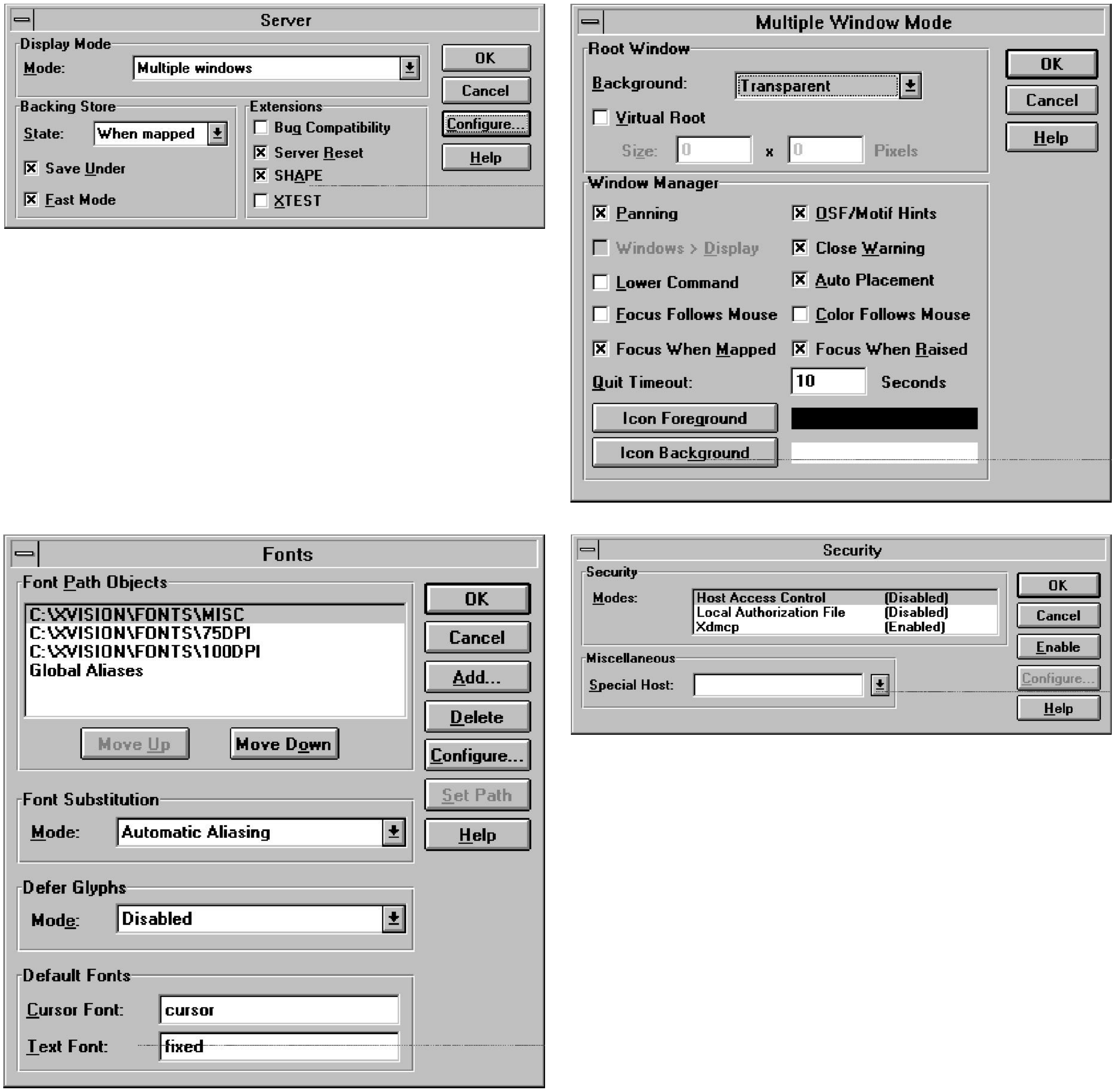
Drawing Optimizations
☒ Treat One-Width Lines as Zero-Width
☒ Eliminate Redundant Rectangles
☒ Pixel Pattern Recognition

Video Driver
☒ Pixmap Banding
☒ Replicate Background Pattern

X Server Memory Usage

Figure 16-4. (2 of 2)

16.1.7 XVision. The Xvision Control Panel allows configuring of the server without starting an X session. Click the right mouse button over the **Xvision Control Panel**. Choose the menu command that contains the option to be changed. Figure 16-5 provides screen captures of the options and selections.



Server

Display Mode
Mode: Multiple windows

Backing Store
State: When mapped
☒ Save Under
☒ Fast Mode

Extensions
☐ Bug Compatibility
☒ Server Reset
☒ SHAPE
☐ XTEST

Multiple Window Mode

Root Window
Background: Transparent
☐ Virtual Root
Size: 0 x 0 Pixels

Window Manager
☒ Panning
☒ OSF/Motif Hints
☐ Windows > Display
☒ Close Warning
☐ Lower Command
☒ Auto Placement
☐ Focus Follows Mouse
☐ Color Follows Mouse
☒ Focus When Mapped
☒ Focus When Raised
Quit Timeout: 10 Seconds
Icon Foreground ■
Icon Background □

Fonts

Font Path Objects
C:\XVISION\FONTS\MISC
C:\XVISION\FONTS\75DPI
C:\XVISION\FONTS\100DPI
Global Aliases

Font Substitution
Mode: Automatic Aliasing

Defer Glyphs
Mode: Disabled

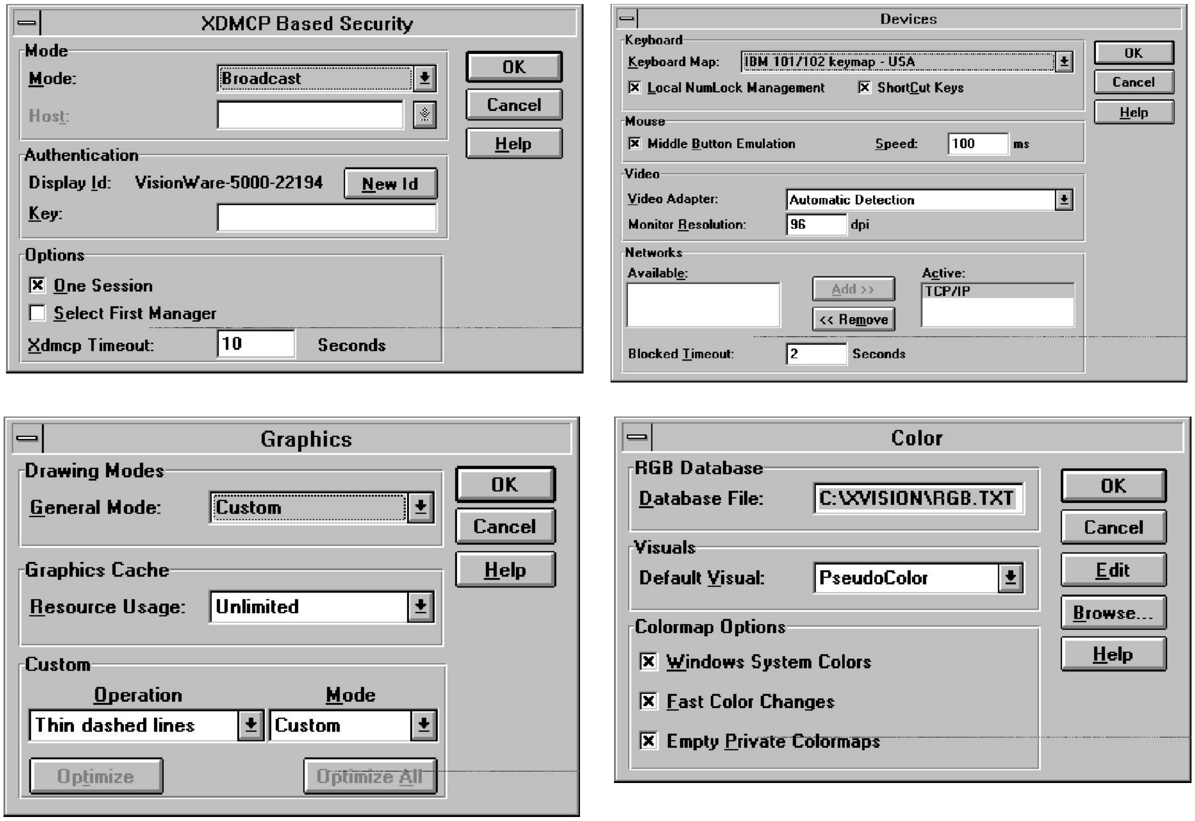
Default Fonts
Cursor Font: cursor
Text Font: fixed

Security

Security
Modes:
Host Access Control (Disabled)
Local Authorization File (Disabled)
Xdmcp (Enabled)

Miscellaneous
Special Host:

Figure 16-5. XVision Screen Captures (1 of 2)



XDMCP Based Security

Mode

Mode: Broadcast

Host:

Authentication

Display Id: VisionWare-5000-22194

Key:

Options

☒ One Session

☐ Select First Manager

Xdmcp Timeout: 10 Seconds

Devices

Keyboard

Keyboard Map: IBM 101/102 keymap - USA

☒ Local NumLock Management ☒ ShortCut Keys

Mouse

☒ Middle Button Emulation Speed: 100 ms

Video

Video Adapter: Automatic Detection

Monitor Resolution: 96 dpi

Networks

Available:

Active: TCP/IP

Blocked Timeout: 2 Seconds

Graphics

Drawing Modes

General Mode: Custom

Graphics Cache

Resource Usage: Unlimited

Custom

Operation	Mode
Thin dashed lines	Custom

Color

RGB Database

Database File: C:\XVISION\RGB.TXT

Visuals

Default Visual: PseudoColor

Colormap Options

☒ Windows System Colors

☒ Fast Color Changes

☒ Empty Private Colormaps

Figure 16-5. (2 of 2)

SECTION 17. BACKUP AND RECOVERY PROCEDURES

The following topics will be included in a later version of the SAM.

17.1 DB Server

17.2 EM Server

17.3 AMHS Server

17.4 DNS Server

17.5 NIS+ Server

17.6 Application Server

SECTION 18. INFORMATION MANAGEMENT SUBSYSTEM/REFERENCE FILE MANAGER (IMS/RFM) ADMINISTRATION

IMS/RFM administration consists of entering the appropriate script names and file paths into config files—one for IMS and one for RFM. The scripts are executed when the IMS and RFM tools are used.

18.1 IMS Admin Tool

The IMS Admin Tool icon launches the IMS configuration function. This function should be used only by designated personnel in accordance with site procedures. IMS controls the Time-Phased Force and Deployment Data (TPFDD) data transfer facility, and is the centralized TPFDD data management interface among DART, JFAST, and the JOPES Core Database.

18.1.1 Who Can Run the IMS Admin Tool. As currently configured, only the user ID who is the owner of the /*h*/*IMS_RFM*/*bin*/*ims_apps* file can start the IMS Admin Tool. By default, the user ID is IMSRM. This means that to use the IMS Admin Tool, a user must log onto it as **IMSRM**.

18.1.2 How to Recover the Original IMS Configuration. If changes need to be made to the IMS operational configuration (the scripts and path names stored in / *h*/*IMS_RFM*/*bin*/*ims_apps* file using the IMS Admin tool), then the user needs to copy the backup file called *ims_apps.real* to the file name /*h*/*IMS_RFM*/*bin*/*ims_apps*.

18.2 RFM

The Reference Manager Administration Tool icon launches the RFM configuration function. To ensure proper management of standard reference files, this function should be used only by designated personnel in accordance with site procedures. RFM is the reference file transfer manager. The Reference Manager icon launches the RFM process, and causes the RFM Command screen to be displayed, for standard reference file transfers. This function should be used only by designated personnel in accordance with site procedures.

RFM allows the user to acquire and transfer JOPES standard reference files (such as ASSETS, CHSTR, GEOFILE, TUCHA) required for operation planning. RFM gets the reference files from the JOPES Core Database when the RFM Update button is used for a given reference file.

18.2.1 Who Can Run the RFM Admin Tool. As currently configured, only the user ID who is the owner of the /*h*/*IMS_RFM*/*files*/*refapp_info* file can start the Refman Admin Tool. By default, the user ID is IMSRM. This means that to use the RFM Admin Tool, a user must log onto it as **IMSRM**.

18.2.2 How to Recover the Original RFM Configuration. If changes need to be made to the RFM operational configuration (the scripts and path names stored in / *h*/*IMS_RFM*/*files*/*refapp_info* file using the RFM Admin tool), then the backup file called *refapp_info.real* must be copied to the file name *refapp_info*.

SECTION 19. AMHS ADMINISTRATION

These are the post-install procedures for the GCCS AMHS Server and Client segment.

19.1 EM Server Procedures

The following procedures are for installation on the platform designated as the EM Server.

a. Add amhserver, alias, and SAT to NIS+ server hosts file:

```
# vi /h/EM/nis_files/hosts
      IP address amhserver
      IP address sat

# cd /h/EM/nis_files/update
# /usr/ccs/bin/make hosts
```

b. Using Security Manager (SM), create the following groups, using these menu selections: File -> Group -> New. Then enter:

Group Name	Group Member
amh_cwp	**200**
amh_fbis	**201**
amh_excl	**203**
amh-limd	**204**
amh_nato	**205**
amh_pers	**206**
amh_spec	**207**
amh_ts	**208**
amh_rel	**209**

c. Using SM, create user account for "amhs_dba", using the menu selections: File -> Create Account. Then enter:

User Id	**amhs_dba**
User Number	**202**
Password	**xxxx**
SYBASE SA Username	**yyyy**
SYBASE SA Password	**zzzz**
Default Group	**gccs**
Optional Group	
Account Group	**GCCS Operator**
Role	**GCCS Default**

d. Assign amhs_dba to groups created in step b, using these menus selections: File -> Groups -> Edit User's Groups.

e. Change home directory for amhs_dba:

```
# nistbladm -m home=/h/AMHS/Server/topic/amhs_db/home
     '[ name=amhs_dba, ],passwd.org_dir'
     ^---Single Quote
```

f. Turn on YP compatibility:

```
# vi /etc/rc2.d/S71rpc
     Uncomment -> #    EMULYP = "Y"
```

g. Install PCNFSD:

Insert diskette (PCNFS - 5 of 5)

```
# volcheck
# cd /floppy/sunpc-nfs/sunos.5x/sparc
# cp pkg.taz /var/spool/pkg
# cp addpkg.taz /var/spool/pkg
# cd /var/spool/pkg
# ./addpkg.sh
# pkgadd
```

If error message:

```
        dup_grp_ent
```

remove nisplus entries for passwd and group in */etc/nsswitch.conf* file, re-run above step and then restore *nsswitch.conf* file.

```
The following packages are available:
        1.  SUNWpcnfs      PC-NFS Daemons
Select package(s) you wish to process ....

Do you want to install the PC-NFS daemon ?  Y

Do you want to install the Console Messaging server ?  N

Do you want to install the PC-NFS licensing ?  Y

Do you want to install the PC-NFS Slip Driver ?  N
```

19.2 AMHS Server Procedures

The following procedures are for installation on the platform that will serve as the AMHS Server:

a. If /amhs does NOT exist; execute the following:

```
# mkdir /amhs
# vi /etc/vfstab
      make entry for amhs from empty filesystem of
      at least 2GB (e.g. home2 --> amhs)
# init 6 ( Reboot)
```

b. **# vi /etc/dfs/dfstab**

Add entry share -F nfs /amhs

c. Execute the following:

```
# cd /amhs
# mkdir sat
# mkdir dac
# mkdir topic
# chown -R amhs_dba *
# chgrp -R gccs *
# chmod -R 775 sat
# chmod -R 775 dac
# chmod -R 775 topic
```

*you should be in /h/AMHS_SRV

d. Execute the following:

```
# su - amhs_dba
> cd /h/AMHS_SRV/sat
> find . -print | cpio -pdmuv /amhs/sat

> cd /h/AMHS_SRV/dac
> find . -print | cpio -pdmuv /amhs/dac

> cd /h/AMHS_SRV/topic
> find . -print | cpio -pdmuv /amhs/topic

> cd ..
> pwd

> su    (to root)
```

```
# rm -r sat
# rm -r dac
# rm -r topic

# ln -s /amhs/sat sat
# ln -s /amhs/dac dac
# ln -s /amhs/topic topic

# cat /h/AMHS_SRV/data/config/active_apt.AMHS >>
    /h/data/global/EMDATA/config/active_spt

# vi /h/data/global/EMDATA/config/active_spt
    Esc
    :1,$s/egret/"amhserver-name"/

# init 6
```

e. Log in as **root**, then execute the following:

# vi /h/data/global/EMDATA/config/processor_table

Add the following entry:

```
amhserver  GCCS  AMHS server
```

```
# cd /h/amhs/sat
# mv autodin autodin.tlc
# mkdir autodin
# chown -R amhs_dba autodin
# chgrp -R gccs autodin
# chmod -R 775 autodin
```

NOTE: The following procedures are for installation on the Standard Automated Terminal (SAT). Execute the following:

edit **A:\HOSTS**

There should be two entries for the EM server; change one of them to values of the AMHS server:

Create **A:\DRIVES.BAT**

```
NET USE J:  amhserver:/amhs/sat  /ms
```

Insert SAT diskette

Copy **A:\*.* J:\autodin**   (17 files copied)

Edit **J:\autodin\sat.ini**

# vi /amhs/sat/autodin/sat.ini

Change:	**MasterPath = E:\(GENSER)**
to:	**MasterPath = J:\autodin**

Execute the following:

```
J:\autodin\setup
```

BASE I/O	300
INTERRUPT	5
WINDOW ADDRESS D	800

f. Log on as *amhs_dba* on AMHS server. Home directory should be */h/AMHS/Server/topic/amhs_db/home*

g. Execute the following:

```
> cd ../amh_admin
```

h. Execute the following:

```
> ./topic_cmd
```

In the AMHS System Admin and Database Admin Commands Main Menu:

i. Enter option **1** (Startup all AMHS processes)

j. Enter **.** to exit

k. Enter **exit** to get back to command prompt.

19.3 Procedures for All AMHS Platforms

The following procedures must be done on all platforms that have AMHS installed:

a. Log on as **root**

b. Execute the following:

```
# /usr/asterix/asterix
```

From the Applix menu select ***** then **Macro Editor**

c. Select **File -> Open**

d. From the "Open" pop-up menu:

Double click on **h**.
Double click on **COTS**.
Double click on **APPLIX**.

Double click on **axlocal**.
Double click on **elf**.
Double click on **mtf_editor**.

e. From the MTF_editor pop-up menu:

1. Select **Find** from the bar menu.

2. Click on **Find & Replace**.

3. Type the following in the "Find" Box:

   usr/edss/mount_point/pla_tables

4. Type the following in the "Replace" Box:

   usr/edss/pla_tables

5. Click on **Replace All**.

6. Close the **Find & Replace** pop-up menu.

7. Select **File** from the menu bar.

8. Click on **Compile & Save**

9. Select **File** from the menu bar.

10. Click on **Exit**.

f. Execute the following:

```
# vi /h/CCAPPS/data/config/Mv.CCA
```

Edit last line:

```
MTF_SITE=..../h/CCAPPS/data/config/Mv.CCA
```

g. Execute the following:

```
# cd /h/data/global/EMDATA/pla_tables
```

h. Execute the following:

```
# vi Ri.CCA
```

RUSNMHS -> RI of ORIGINATOR
RUSNSUU -> RI of PRIMARY ADDRESSEE

i. Execute the following:

```
# vi Class.CCA
```

Remove TOP SECRET Information.

j. Execute the following:

```
# vi MAST_PLA.CCA
```

Make any needed changes.

k. Execute the following:

```
# /h/CCAPPS/progs/create_pla_files
```

l. Execute the following:

```
# mkdir /h/data/global/EMDATA/amhs_install
```

m. Execute the following:

```
# cp /h/COTS/APPLIX/axlocal/elf/mtf_editor.am
   /h/data/global/EMDATA/amhs_install
```

19.4 AMHS Client Platform Procedures

The following procedures are designated for all AMHS CLIENTS platforms:

a. Log in as **root**.

b. Execute the following:

```
# vi /etc/vfstab
```

The following line should be there:

```
amhserver:/h/AMHS_SRV - /h/AMHS/Server nfs - yes rw,bg,soft
```

Add the following line:

```
amhserver:/amhs  - /amhs  nfs  -  yes rw,bg,soft
```

c. Execute the following:

```
# mkdir /amhs
```

d. Execute the following:

```
# mount /amhs
```

e. Execute the following:

```
# cp /h/data/global/EMDATA/amhs_install/mtf_editor.am
  /h/COTS/APPLIX/axlocal/elf/
```

f. Execute the following:

```
# vi /h/CCAPPS/data/config/Mv.CCA
```

Edit last line:

```
MTF_SITE=..../h/CCAPPS/data/config/Mv.CCA
```

SECTION 20. CHANGING IP ADDRESSES AND HOST NAMES

20.1 Changing IP Addresses on SPARCstations

When a site finds it necessary to change the IP address of a SPARCstation(s), there are several files both on the affected SPARCstation and on other platforms that may require modification. Perform the following steps using the editor of your choice on the SPARCstation for which the IP address is being changed:

a. Deactivate NIS+ on the SPARCstation by executing the following (see also Section 6 of this Manual):

```
# cd /var/nis<return>
# rm -rf * <return>
# rm /etc/defaultdomain <return>
# rm /etc/.rootkey <return>
# ps -ef | grep nis <return>
```

Note the process ID (PID) for :

```
/usr/sbin/rpc.nisd -r
/usr/sbin/nis_cachemgr
```

```
# kill -9 {PID} {PID}<return>
```

b. If changing the IP address of the ORACLE database server, de-install the DART application.

c. In the */etc/inet/hosts* file change the IP address for the SPARCstation being modified.

Example: 164.117.210.166 brady

d. In the */etc/inet/netmasks* file, change the network number and the netmask if necessary. Both numbers are written in "decimal dot" notation and should be obtained from your network administrator.

Example: 164.117.0.0 255.255.255.0

e. In the */etc/inet/networks* file, change the broadcast address to that of the Executive Manager.

Example: subnet1.gccs 164.117.210.255

This address can be determined by running the following command on the EM server:

ifconfig ??? where ??? is the ethernet port number of SPARCStation, e.g., le0, ie0

f. If the IP address of the default router has changed, modify the following file accordingly:

/etc/defaultrouter

g. If the IP address and/or the DNS domain name have changed, modify the *\/etc/resolv.conf* to reflect this.

   Example: domain ims.disa.mil
   namserver 164.117.210.64

h. Re-boot the system.

i. If this is the ORACLE database server, install the DART application.

j. Refer to Section 20.3 for changes required to NIS+ and DNS.

20.2 Changing the Host Name of a SPARCstation

When it is necessary to change the host name of a SPARCstation(s) there are several files both on the affected SPARCstation and on other platforms that may require modification. Perform the following steps using the editor of your choice on the SPARCstation whose host name is being changed:

a. Deactivate NIS+ on the SPARCstation by executing the following (see also Section 6 of this Manual):

```
# cd /var/nis<return>
# rm -rf * <return>
# rm /etc/defaultdomain <return>
# rm /etc/.rootkey <return>
# ps -ef | grep nis <return>
```

   Note: the process ID (PID) for:

```
/usr/sbin/rpc.nisd -r
/usr/sbin/nis_cachemgr

kill -9 {PID} {PID}<return>
```

b. If changing the host name of the ORACLE database server, de-install the DART segment.

c. In the */etc/inet/hosts*, file change the host name for the SPARCstation being modified.

   Example: 164.117.210.166 brady

d. In the */etc/nodename* file, change the host name entry to the new host name.

e. In the */etc/hostname.???* (where ??? is the ethernet port of the SPARCstation, e.g., /etc/hostname.1e0) change the host name entry to the new host name.

f. In the */etc/net/ticlts/hosts* change all occurrences of the old host name to the new host name.

g. In the */etc/net/ticots/hosts* change all occurrences of the old host name to the new host name.

h. In the */etc/auto_home* file change all occurrences of the old host name to the new host name.

i. Execute the following:

```
# mv  /.xsun.{old hostname}:0  /.xsun.{new hostname}:0
```

j. All occurrences of the old host name in the users *.rhosts* file will have to be changed to the new host name. The *.rhosts* are located in the following directories:

```
/h/USERS/{user id}/Scripts
```

k. If changing the host name of the Executive Manager server changes any occurrence of the old host name to the new host name in the following files:

```
/h/EM/admin/security-scripts/security-servers
/h/data/global/EMDATA/config/active_spt
/h/data/global/EMDATA/config/processor_table
```

l. Re-boot the system.

m. Refer to Section 20.3 for changes required to NIS+ and DNS.

n. If this is the ORACLE database server, install the DART segment at this point.

20.3 Changes Required to NIS+ and DNS when Changing Host Names and IP Addresses

After all the system files have been modified on the SPARCstation whose IP address and/or host name is being changed the NIS+ database will have to be update to reflect the change. To do this, execute the procedures in Section 6.2.3 of this Manual, "Setup NIS+ on Client."

If the IP address of the NIS+ server has been changed the NIS+ server will have to be reconfigured (see Section 6.2.1 of this Manual), as will all the clients.

Any change of a host name and/or IP address requires a change to the DNS nameserver database. Consult Section 5 of this Manual "DNS Administration" for the procedures on modifying the nameserver tables.

20.4 Changing IP Address and/or Host Name on Sybase Server

If the host name and/or IP address of the Sybase server is changed, the "interfaces" file located in */h/COTS/SYBASE* must be updated, since it contains both the host name an IP address (in hexadecimal). To do this, execute the following on the Sybase server:

a. Log in as **root** and change the host name of the Sybase server found in the */etc/inet/hosts* to a dummy name.

b. Add the new IP address of the Sybase server followed by the host name to the */etc/inet/hosts* file.

c. Execute the following:

```
# su - sybase<return>
# cd /h/COTS/SYBASE/install<return>
```

d. Modify the IP address by executing the following:

```
# sybinit<return>
```

The following output will appear:

```
The log file for this session is
'/home1/COTS/SYBASE/init/logs/log0801.001'.

SYBINIT

1. Release directory:    /h/COTS/SYBASE

2. Edit  /  View Interfaces File

3. Configure a Server product
4. Configure an Open Client/Server product


Ctrl-a Accept and Continue,  Ctrl-x Exit Screen,  ?  Help.

Enter the number of your choice and press return:
```

e. Enter the following:

2 (Edit / View Interfaces File)

followed by a <return>.

The following output will appear:

```
INTERFACES FILE TOP SCREEN

Interfaces File:

1. Add a new entry
2. Modify an existing entry
3. View an existing entry
4. Delete an existing entry


Ctrl-a  Accept and Continue,  Ctrl-x Exit Screen,  ?  Help.
```

```
Enter the number of your choice and press return:
```

f. Enter the following:

2 (Modify an existing entry)

followed by a <return>.

The following output will appear:

```
CHOOSE INTERFACES FILE ENTRY

Select one of the following interfaces entries:

1. SYB_BACKUP
2. GCCS

Ctrl-a  Accept and Continue,  Ctrl-x Exit Screen,  ?  Help.

Enter the number of your choice and press return:
```

g. Enter the following:

1 (SYB_BACKUP)

followed by a <return>.

The following output will appear:

```
SERVER INTERFACES FILE ENTRY SCREEN

   Server name:    SYB_BACKUP

1. Retry Count:    0
2. Retry Delay:    0

3. Add a new listener service

Modify or delete a service

Listener services available:

   Protocol  Address      Port      Name Alias
4. tcp       brady        6500


Ctrl-a Accept and Continue, Ctrl-x Exit Screen,  ?  Help.

Enter the number of your choice and press return:
```

h. Enter the following:

4 (Protocol Address Port Name Alias)

followed by <return>.

The following output will appear:

```
EDIT TCP SERVICE

1. Hostname/Address:  brady
2. Port:  6501
3. Name Alias:

4. Delete this service from the interfaces entry


Ctrl-a Accept and Continue, Ctrl-x Exit Screen,  ?  Help.

Enter the number of your choice and press return:
```

i. Enter the following:

1 (Hostname/Address)

followed by <return>.

The following output will appear:

```
Enter the hostname or Internet address to use for this entry
(default is 'brady'):
```

j. Enter the following:

{IP address}

or

{hostname}

followed by a <return>.

The following output will appear:

```
1. Hostname/Address:  hostname
2. Port:  6501
3. Name Alias:

4. Delete this service from the interfaces entry
```

```
Ctrl-a Accept and Continue, Ctrl-x Exit Screen,  ?  Help.

Enter the number of your choice and press return:
```

k. Enter:

Ctrl-a (Accept).

l. Enter:

Ctrl-x

m. Enter the following:

Ctrl-x

The following output will appear:

```
CHOOSE INTERFACES FILE ENTRY

Select one of the following interfaces entries:

1. SYB_BACKUP
2. GCCS

Ctrl-a  Accept and Continue,  Ctrl-x Exit Screen,  ?  Help.

Enter the number of your choice and press return:
```

n. Enter the following:

2 (GCCS)

followed by a <return>.

The following output will appear:

```
SERVER INTERFACES FILE ENTRY SCREEN

   Server name:    SYB_BACKUP

1. Retry Count:    0
2. Retry Delay:    0

3. Add a new listener service

Modify or delete a service

Listener services available:
   Protocol  Address      Port      Name Alias
4. tcp       brady        6500

Ctrl-a Accept and Continue, Ctrl-x Exit Screen,  ?  Help.

Enter the number of your choice and press return:
```

o. Enter the following:

4 (Protocol Address Port Name Alias)

followed by <return>.

The following output will appear:

```
EDIT TCP SERVICE

1. Hostname/Address:  brady
2. Port:  6501
3. Name Alias:

4. Delete this service from the interfaces entry

Ctrl-a Accept and Continue, Ctrl-x Exit Screen,  ?  Help.

Enter the number of your choice and press return:
```

p. Enter the following:

1 (Hostname/Address)

followed by <return>.

The following output will appear:

```
Enter the hostname or Internet address to use for this entry
(default is 'brady'):
```

q. Enter:

the new **IP address** or **hostname**

followed by a <return>.

The following output will appear:

```
1. Hostname/Address:  hostname
2. Port:  6501
3. Name Alias:
```

```
4. Delete this service from the interfaces entry

Ctrl-a Accept and Continue, Ctrl-x Exit Screen,  ?  Help.

Enter the number of your choice and press return:
```

r. Enter the following:

Ctrl-a (Accept).

s. Enter the following:

Ctrl-x

until the command line prompt is displayed.

t. Type:

exit

to return to root.

u. Execute the following on the new *interfaces* file to make it available to all GCCS platforms:

```
# cp  /h/COTS/SYBASE/interfaces  /h/data/global/EMDATA/sybase
```

v. In the */h/COTS/SYBASE/install/gccs.rs* file change the host name entry at the end of the following line:

```
sqlsrv.network_hostname_list: {hostname}
```

w. In the */h/COTS/SYBASE/install/gccs_Backup.rs* file change the host name entry at the end of the following line:

```
bsrv.network_hostname_llist: {hostname}
```

x. Change any occurrance of the old host name to the new host name in the following files:

```
/h/data/global/EMDATA/config/active_spt
/h/data/global/EMDATA/config/processor_table
```

SECTION 21. UPS ADMINISTRATION

Uninterruptible Power Supply (UPS) systems are designed to provide AC input power protection to attached equipment, against a variety of irregular power conditions. These power conditions can range from power spikes to a total power outage, causing hardware damage or loss/corruption of data.
To mitigate administration down-time in the event of a unwanted power condition as described above, UPSs have been provided.

Effectively providing reliable power conditioning for a system requires that the total system load requirements must first be determined. Once system load and power consumption has been determined, the correct UPS model can be selected to provide regulated and filtered incoming AC power to the attached system. This is accomplished by identifying all equipment that must have power protection, and the peak power consumption for each device as specified by the equipment manufacturer. For the known various GCCS configurations, the recommended configuration is that the UPS connected to the CPU should also have connected to it the monitor and as many primary external support drives as possible. After determining the best possible configuration for the system connections, proceed to Section 21.2, "Hardware Installation."

21.1 Related Documents

- UPSI Operations Manual
- OnliSafe Power Manual

21.2 Hardware Installation

This section will guide the installer through unpacking and operational configuration of the UPSI UPS 800ext-1500ext models.

1. ***** IMPORTANT ***** Read the safety instructions contained on pages 7-9 in the *UPSI Operations Manual*.

2. Unpack and inspect the UPS as described on page 41 of the *UPSI Operations Manual*.

3. Connect the power cord to the UPS input power connector located on the rear panel of the UPS. Do not connect the power cord(s) of the protected equipment into the power output receptacles at this time. Plug the UPS power cord into a grounded house power receptacle and watch the UPS control panel indicators. After the UPS cycles through internal power up diagnostics, indicators I1 (green) and I7 (amber) will remain illuminated (see Figure 21.1). This condition indication is normal UPS operational condition exists. If the UPS does not switch to the normal operational mode immediately remove AC input power from the UPS and refer to the Error Conditions section on page 53 in the *UPSI Operations Manual*.

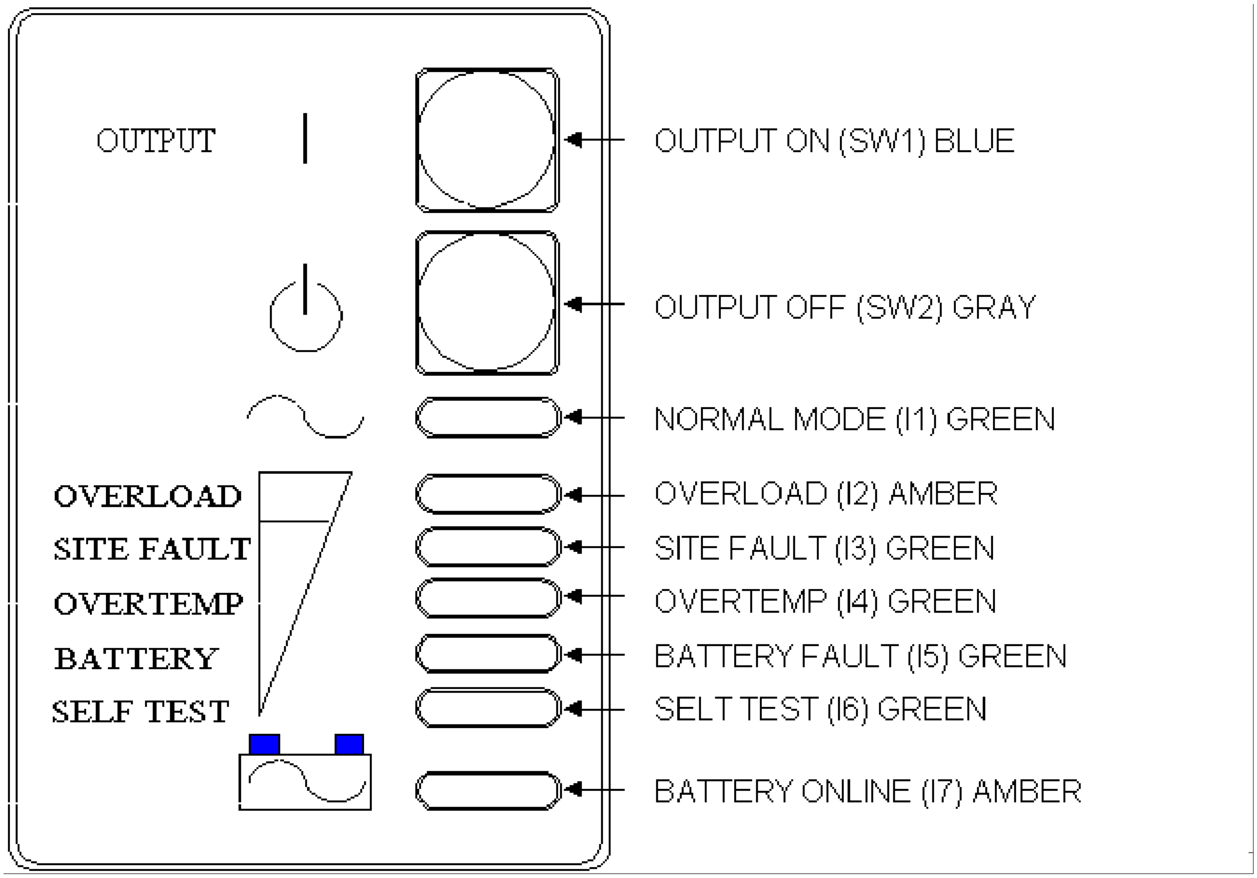


Figure 21-1. UPS Front Panel Controls and Indicators

4. The UPS is equipped with an external communications port used to communicate with the SPARC computer running OnliSafe power management software. To allow computer to UPS communications will require reconfiguration of the UPS communications port from the factor default configuration. The steps provided below will reconfigure the UPS port to the AS/400 configuration. It is recommended that the installer reviews the steps below before proceeding with the installation. The UPS has a configuration time limit, which, if exceeded, will require the steps to be performed repeatedly until performed correctly in a timely manner.

   a. Unplug the UPS AC input power from house power.

   b. Plug the UPS AC input power into house power while pressing the UPS Output OFF (SW2) on the UPS front panel until the alarm beeps (see Figure 21.1). All indicators will begin to flash on and off.

   c. Immediately press the Output OFF (SW2) on the UPS front panel until the alarm beeps again. The I3 factor default configuration indicator will begin to flash on and off.

d. Immediately press the Output OFF (SW2) on the UPS front panel one time or repeatedly until the I4 indicator begins to flash on and off.

e. Immediately press the Output ON (SW1) on the UPS front panel until the alarm beeps, and then press the Output ON (SW1) a second time. The UPS will switch to the normal operational mode.

f. The configuration can be verified by performing Steps a through c again.

g. After successful completion of the hardware installation, the protected equipment can be plugged into the power output receptacles located on the rear of the UPS.

h. Proceed to Section 21.3, OnliSafe Powerware Software Installation.

NOTE: If the site needs further assistance, contact:

Universal Power Systems, Inc.
11200 Waples Mill Road, Suite 350
Fairfax, Virginia 22030
(800) 438-8774
(703) 352-8644

21.3 OnliSafe Powerware Software Installation

The UPS is equipped with a communications port used to communicate with computers running OnliSafe power management software. The power management software has been preconfigured and segmented for installation onto a GCCS SPARC system running Solaris 2.3/SunOS 5.3. Prior to installing the UPSI Segment Version 1.3, "Powerware OnliSafe Solaris (SPARC) V 3.1.2 software," the installation instructions in Section 21.2, "Hardware Installation," should be performed. If the hardware installation has not been implemented, the system should be shut down and disconnected from the UPS, and the installation instructions in Section 21.2 "Hardware Installation" should be performed. After hardware installation, the segment installation can be performed following the steps described in Section 3, "Segment Installer."

a. Plug the CT-03-92M RS-232 cable provided with the UPS software into the UPS and the computer.

NOTE: Special care should be taken to identify the cable ends labeled CPU and UPS. If cable ends are reversed the computer will power up and then start the power shutdown sequence because it can not verify the presence of the UPS.

The CPU end of the communication cable should be plugged into the TTY/A port on the SPARC computer. If this port is not available, the OnliSafe power management software will require reconfiguration as described on pages 8 through 16 of the OnliSafe Power Manual.

b. Install the UPSI Segment using the GCCS segment installer. The only modification to the software configuration other than that noted above is related to the shutdown procedure used to shut down the system during a power outage. The default software shutdown procedures for a power outage are that the system shuts down and re-boots until power has been restored or until the UPS battery has been completely drained of power and no longer can re-boot. To modify the shutdown procedure to keep the system from attempting to re-boot:

1. Change the UPSI segment scripts directory:

```
# cd /h/COTS/UPSI/scripts
```

2. Edit the shutdown script.

```
 # vi power_mon.hlt2
```

3. Edit the last line in the file to read:

```
# cd /;uadmin 2 0 > /dev/console 2>/dev/console
```

c. After the software segment installation is completed, the system will require a system shutdown and reboot to activate the power management software.

NOTE: If the site needs further assistance, contact:

Exide Electronics
8521 Six Forks Roads
Raleigh, North Carolina 27615
(919) 870-3300

SECTION 22. EXECUTIVE MANAGER OPERATIONS

NOTE: The Executive Manager (EM) is continually being revised. Consequently the documentation in this section is a "snapshot" of the EM procedures for a particular version. There may be differences after patches are applied during the course of GCCS Version 2.1 installation.

22.1 Introduction

The System Administrator (SA) maintains control of the GCCS Desktop by providing user profiles, assigning privileges to each user, and the granting of access to system and application resources. The structure of the SA's desktop is provided in Figure 22-1.

The SA (or its designated authority, such as the Security Administrator), through the use of the Executive Manager's five programs, i.e., Security Manager, Profile Manager, Role Manager, Monitor, and Control Manager, provides the following services:

- User account maintenance: creating new accounts; modifying existing accounts; deleting existing accounts; and defining and viewing various audit logs and viewing lists of special access categories associated with users.

- System profile maintenance: adding/deleting/changing user profiles and projects.

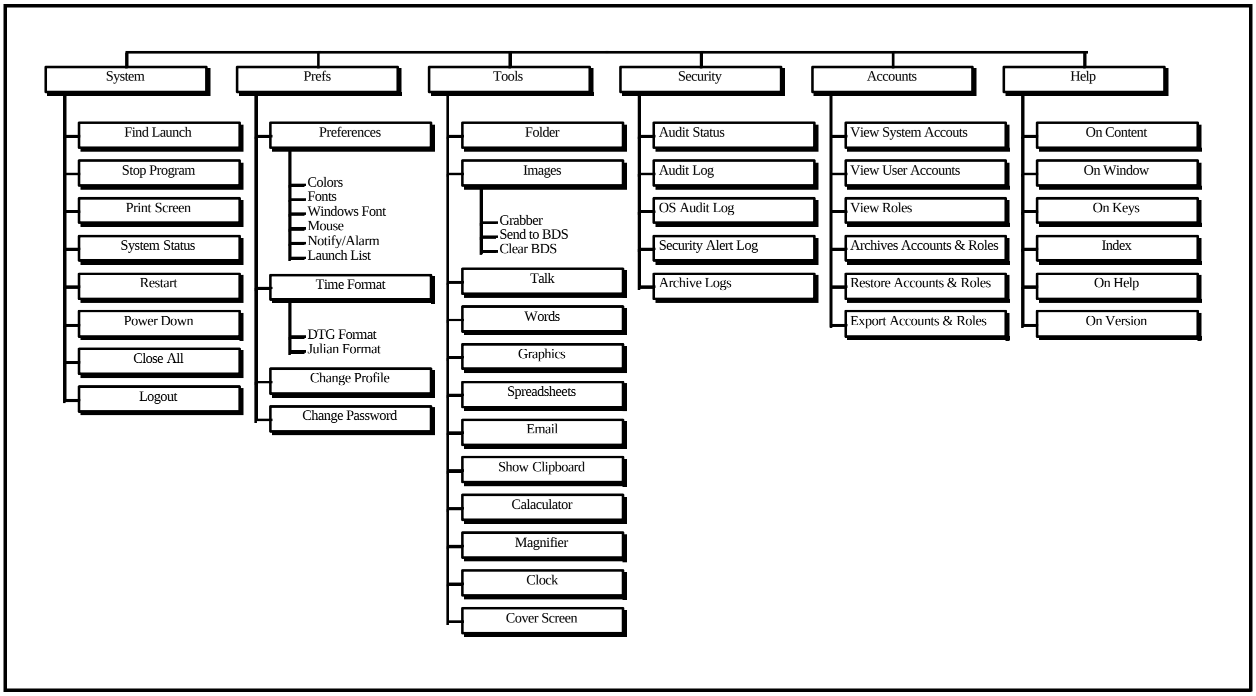


Figure 22-1. System Administrator's Desktop Menu Structure

Profiles contain information related to a user's administrative chain of command (reporting path) and permissions to access specific GCCS applications. Profile attributes consist of: Project, Position, Directorate, Division, Branch, Section, and Cell, which represent organized structures as well as folder (directory) structure access. The profile attributes have modifiers to notify the user of messages related to the user's administrative structure and folder/file handling privileges. Profiles exist only when associated with a specific user. Profiles contain a list of applications available to that specific user. That list is known as a Launch List.

Attribute modifiers are Delete rights and Notify rights. The Delete right will permit the user to delete folders and folder elements contained in the selected organization's folder. The Notify right indicates that the specific user will be informed when messages are received for that organization.

22.2 User Account Maintenance

User account maintenance is performed by the SA using the GCCS Desktop’s Security Manager. (The menu structure of the Desktop's Security Manager is provided in Figure 22-2). The Security Manager is a user-interactive program that allows the SA to create new accounts, modify existing accounts, delete existing accounts, define and view various audit logs, and view lists of special-access category AMHS messages.

Audit logs are files generated automatically by the GCCS system to save a journal of system activity performed by any user logged on to the system. There are two kinds of audit logs: UNIX logs and Database logs.

Special-access categories are specific privileges associated with the ability of a user to perform operations, create, delete, and view AMHS messages ("limdis," "exclusive," etc.)

22.2.1 Security Manager Activation. To activate the Security Manager program:

a. Click twice in rapid succession on the **SECURITY** icon on the Session Manager's Launch Window. The "run_security" window is displayed.
b. Enter password. Upon successful program initialization, the Security Manager main window is displayed.

22.2.2 Security Manager Termination. To exit the Security Manager:

a. Click on **File > Exit** on the "Security Manager" menu bar. A prompt will confirm the exit request.

b. Click on **OK**. All Security Manager-related windows vanish.

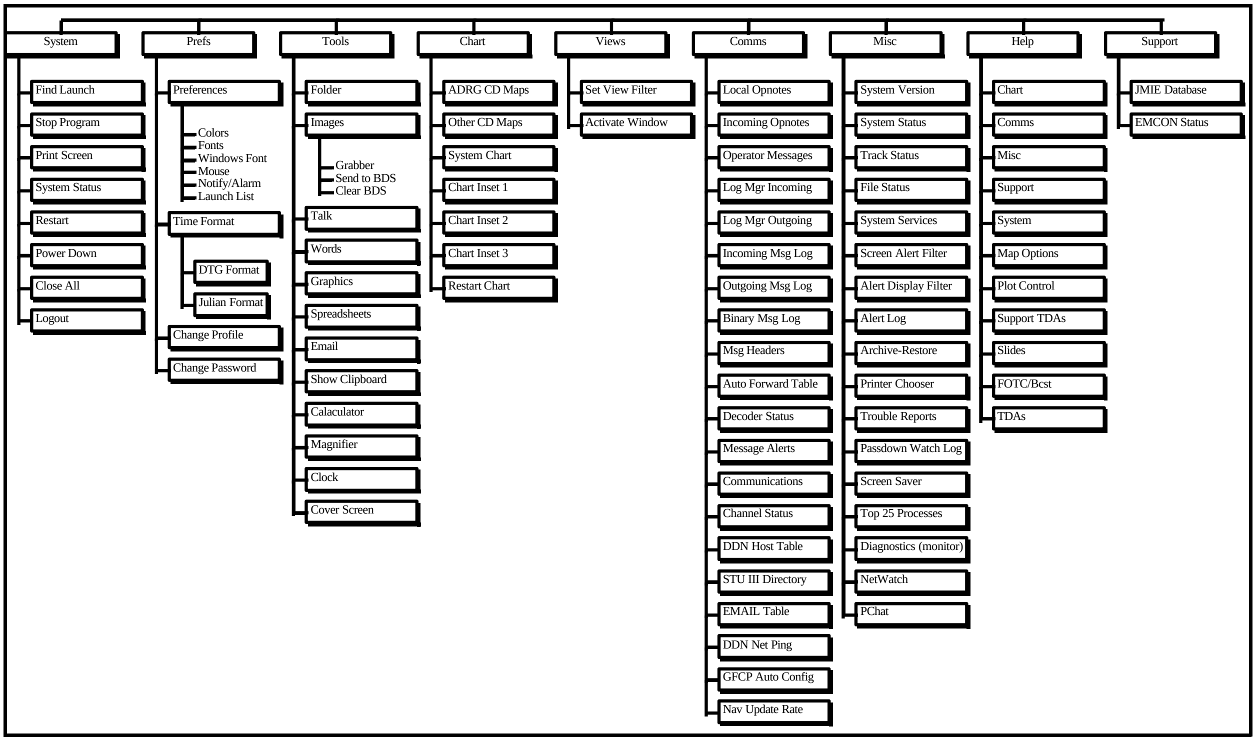


Figure 22-2. Security Manager's Desktop Menu Structure

22.2.3 Security Main Window. The Security Manager main window has the following menus on the menu bar (see Figure 22-3): "File," "Edit," "Options," and "Help." Options available in each menu are shown in Figure 22-4.

In the Security Manager main window there is listed for each account a "Userid," "Num," "D-Group," "Username," and "Group" (see Figure 22-3). D-Group represents the default group, and Group represents any other groups to which the user also retains privileges.

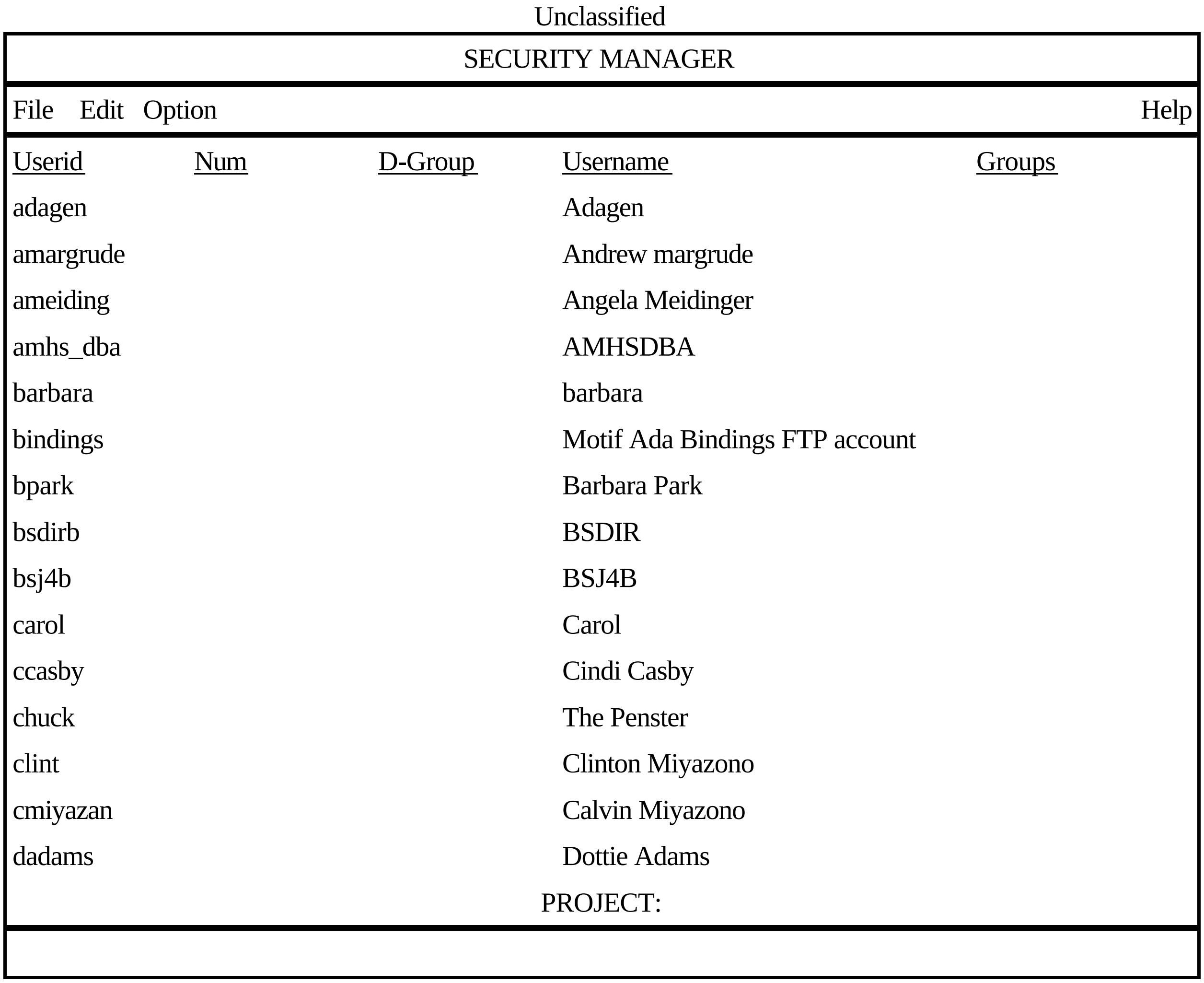
22.2.4 User Account Maintenance Tasks. The following paragraphs provide the necessary step-by-step actions required to utilize the capabilities provided by the Security Manager to perform user account maintenance tasks.

a. **Creating a New Account.** To create a new user account:

1. Activate the Security Manager, as described in paragraph 22.2.1.

2. Click on **File > Create Account** on the "Security Manager" menu bar. The "Security Manager:Create User" window is displayed.

3. Type in all the text fields, including the Sybase System Administrator account password. The password is not visible during type-in.



Unclassified

SECURITY MANAGER

Userid	Num	D-Group	Username	Groups
adagen			Adagen	
amargrude			Andrew margrude	
ameiding			Angela Meidinger	
amhs_dba			AMHSDBA	
barbara			barbara	
bindings			Motif Ada Bindings FTP account	
bpark			Barbara Park	
bsdirb			BSDIR	
bsj4b			BSJ4B	
carol			Carol	
ccasby			Cindi Casby	
chuck			The Penster	
clint			Clinton Miyazono	
cmiyazan			Calvin Miyazono	
dadams			Dottie Adams	

PROJECT:

Figure 22-3. Security Manager Main Window

4. Click on the special-access categories that this user will have, then click on **Ok/Apply**. The new user account is added to the main window, in alphabetic order, with all the special access categories assigned to it. The newly created account is available for logon at this time.

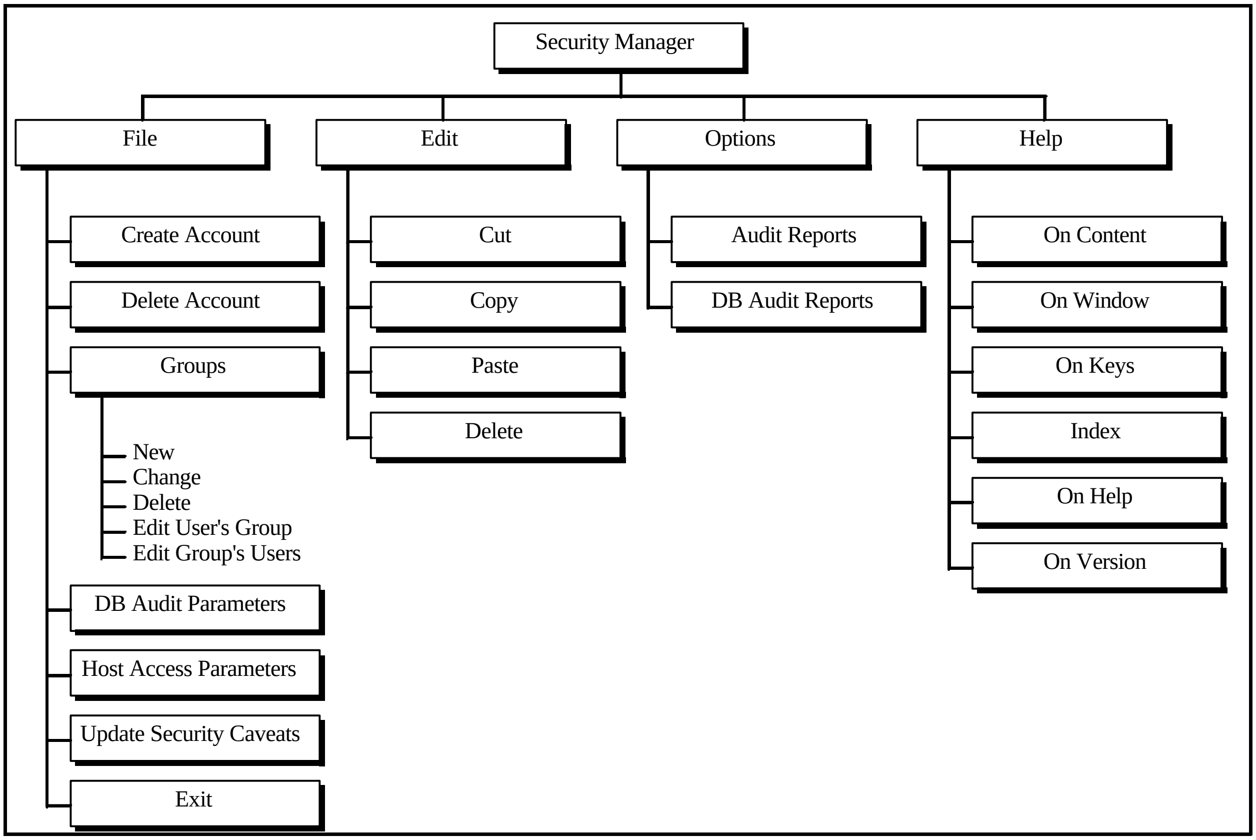


Figure 22-4. Security Manager Menu Structure

b. **Deleting an Account.** To delete an account:

1. Click on an account to be deleted from the Security Manager main window. The selected account is highlighted.

2. Click on **File > Delete Account** on the Security Manager menu bar. The "Security Manager:Delete Account" window is displayed.

3. Type in the Sybase System Administrator account password. The password is not visible during type-in.

4. Click on **yes** or **no** in response to the "Delete User Directories and Files" question.

5. Click on **Ok/Apply**. The selected account is deleted from the main window. The duration of the delete process may vary according to the answer in step (4) above. The deleted account is now no longer available for logon.

22.2.5 Group Maintenance Tasks. The following paragraphs provide the necessary step-by-step actions required to utilize the capabilities provided by the Security Manager to perform group maintenance tasks. The tasks are: creating a new group, deleting a group, editing user groups, and editing groups users.

A. **Creating a New Group.** To create a new group:

1. Activate the Security Manager as described in paragraph 22.2.1.

2. Click on **File > Groups > New** on the “Security Manager” menu bar. The "Security Manager:Create Group" window is displayed.

3. Type in all the text fields, and click on **Ok**.

B. **Changing Group.** To change a group name:

1. Activate the Security Manager as described in paragraph 22.2.1.

2. Click on **File > Groups > Change** on the “Security Manager” menu bar. The "Security Manager: Create Group" window is displayed.

3. Type in all the text fields and click on **Ok**.

> **NOTE:** If a selection arrow box is to the right of a text field, clicking on the arrow will provide a list of available items. Select one and click on **Ok**; the selection is automatically entered for that field.

4. Rename the Group as desired. Click on **Ok**.

C. **Deleting a Group.** To delete a group:

1. Activate the Security Manager as described in paragraph 22.2.1.

2. Click on **File > Groups > Delete** on the “Security Manager” menu bar. The "Security Manager: Delete Group" window is displayed.

3. Type in all the groups and click on **Ok**.

> **NOTE:** If a selection arrow box is to the right of a text field, clicking on the arrow will provide a list of available items. Select one and click on **Ok**; the selection is automatically entered for that field.

4. Click on **Ok**.

D. **Editing User Groups.** To change the groups a user is associated with:

1. Activate the Security Manager as described in paragraph 22.2.1.

2. Click on **File > Groups > Edit User’s Groups** on the “Security Manager” menu bar. The "Security Manager: Edit By User” window is displayed.

3. Type in text fields and click on **Ok**.

> **NOTE:** If a selection arrow box is to the right of a text field, clicking on the arrow will provide a list of available items. Select one and click on **Ok**; the selection is automatically entered for that field.

4. This window will provide a window showing “Assigned Groups” and a window showing “Available Groups.” Clicking on an item in either window will transfer that item to the opposite window, thereby either adding or deleting a group assignment for that user.

5. Click on **Ok**.

E. **Editing a Group’s Users.** To add or delete users within a group:

1. Activate the Security Manager as described in paragraph 22.2.1.

2. Click on **File > Groups > Change** on the “Security Manager” menu bar. The "Security Manager: Edit by Group" window is displayed.

3. Type in text fields and click on **Ok**.

> **NOTE:** If a selection arrow box is to the right of a text field, clicking on the arrow will provide a list of available items. Select one and click on **Ok**; the selection is automatically entered for that field.

4. This window will provide a window showing “Users in Group” and a window showing “Available Users.” Clicking on an item in either window, will transfer that item to the opposite window, thereby either adding or deleting a user in a group.

5. Click on **Ok**.

22.2.6 Audit Monitoring. This capability allows the SA to obtain UNIX audit logs and GCCS Desktop Database audit logs.

22.2.6.1 Setting DB Audit Parameters. This capability allows the SA to set the operating parameters for the GCCS Desktop database audit daemon. The setting of parameters entails selecting table operation(s) to be audited on the GCCS Desktop database tables, and audits of login and logoff attempts. To set DB Audit Parameters:

A. Click on **File > DB Audit Parameters** on the Security Manager menu bar. The "Security Manager:Database Audit Parameters" window is displayed. Note that the window contains a list of all the GCCS Desktop database tables and operations representing the various audit operations.

B. Click on the user for whom the audit parameters are to be set.

C. Click on the table name for the audit parameters to be set. The name of the selected table is highlighted.

D. Click on any combination of operations—Retrieve, Update, Insert, Delete—in the "Security Manager:Database Audit Parameters" window. As each of the operations is selected, the first letter of the operation appears in the Code column corresponding to the selected table name in Step c above.

E. Click on **Auditing Off** in the "Security Manager:Database Audit Parameters" window. The button label changes to "Auditing On." This is a required step if auditing of database operations is desired. Note that the default is "Auditing Off."

F. If auditing of logins is desired, click on **Logins Off** in the "Security Manager:Database Audit Parameters" window. The button label changes to "Logins On." Note that the default is "Logoffs Off."

G. Click on **Reset** in the "Security Manager:Database Audit Parameters" window if all the selections made in steps b through f are to be cancelled.

H. Click on **Apply** in the "Security Manager:Database Audit Parameters" window if all the selections made in steps b through f are to be saved. An audit trail will be available to view through "Option > Unix Audit Logs," and "Option Database Audit Logs" on the Security Manager menu bar.

22.2.6.2 Viewing UNIX Audit Logs. This option allows the SA, with default to the last 24 hours, to display a UNIX system log for each of the following (one at a time): All Logins, Failed Logins, Privileged Commands, and Unauthorized Access. To obtain a UNIX audit log display, do the following:

A. Click on **Option > Audit Reports** on the Security Manager menu bar. The "Security Manager:Unix Audit Display" window is displayed. Note that the period of audit is the last 24 hours.

B. Click on the type of audit log to be displayed by clicking on one of the following options:

- All Logins
- Failed Logins
- Privileged Commands
- Unauthorized Access.

C. Click on **Display** in the "Security Audit Reports" window. The selected, audit log type in step b is displayed.

D. Repeat steps b and c for each audit log type.

22.2.6.3 Viewing Database Audit Logs. This option allows the SA, with default to the last 24 hours, to obtain a GCCS Desktop Database log. The log contains the date, event, user name and pass/fail indication for the event. To obtain a GCCS Desktop database audit log:

A. Click on **Option > Database Audit Reports** on the Security Manager menu bar. The "Security Manager:DB Audit Display" window is displayed. Note that the period of audit is the last 24 hours.

B. Set the correct audit period within the “From Dtg” and “To Dtg” areas and click on Display in the "Security Manager:Database Audit Display" window. The log containing the audit trail is displayed.

C. Click on Print in the "Security Manager:Database Audit Display" window if a printout of the audit log is desired.

22.2.7 Updating Security Caveats. This capability allows the SA to update the security caveats list by adding new or deleting existing security caveats. To update the security caveats list:

A. Click on **File > Update Security Caveats** on the "Security Manager" menu bar. The "Security Manager-Update Security Caveats" window is displayed.

1. To add a caveat:

a. Type in the name of the new caveat in the Caveat Name text area in the bottom of the "Security Manager:Edit Caveats."

b. Click on **Add** in the "Security Manager:Edit Caveats" window. The new caveat name is added to the end of the existing list.

2. To delete a caveat:

a. Click on the name of the caveat, in the existing list, to be deleted. The selected name is highlighted and it appears in the Caveat Name text area in the bottom of the "Security Manager:Edit Caveats" window.

b. Click on **Delete** in the "Security Manager-Edit Caveats" window. The selected caveat name disappears from the existing caveats list.

22.2.8 Setting Access Parameters. This capability allows the SA to set or view host processors available to GCCS at a particular site. To set or view host access:

A. Click on **File > Host Access Parameters** on the Security Manager menu bar. The "Security Manager:Host Access Parameters [GCCS]" window is displayed. Note that the window consists of a list of hosts available and a host access list.

B. Click on **File > Open Access File** in the "Security Manager:Host Access Parameters [GCCS]" window.

C. Select the GCCS platform containing the desired file.

D. Click on **Apply** in the “Security Manager:Open Access File” window.

E. Click the desired host on the "Host Available List" to select a host.

F. Click in the Host Access List to choose specific access parameters.

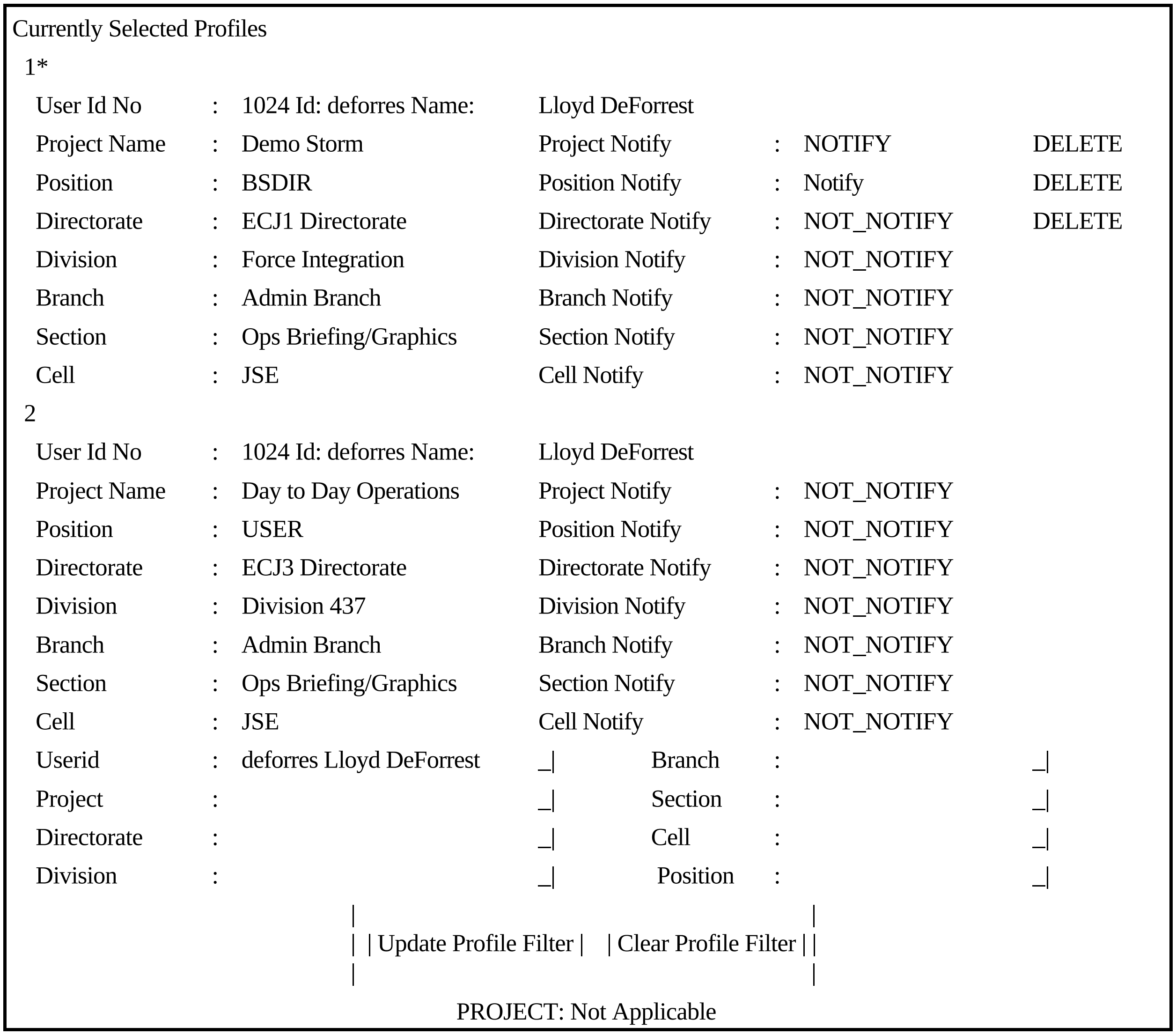
22.3 System Profile Maintenance

System Profile Maintenance is performed by the SA using the GCCS Desktop Profile Manager. The Profile Manager is an interactive program that is used to manage user profile information. This program resides on the GCCS Desktop Dedicated Processor and is started via the Session Manager launch window. The Profile Manager performs the following functions:

- Creates/modifies/deletes profile attributes
- Creates/modifies/deletes new user profiles
- Modifies user's Launch List
- Displays existing users based on profiles.

22.3.1 Profile Description. The construction of a profile for a particular user requires certain profile attributes to be available for (or created prior to) insertion into a profile. These attributes are Project, Position, Directorate (optional), Divisions (optional), Branch (optional), Section (optional), and Cell (optional). If the optional attributes exist, they must also be included.

22.3.1.1 Profile Manager Activation. Click twice in rapid succession on the **PROFILE** icon on the Session Manager's launch window. Upon successful program initialization, the Profile Manager main window is displayed, as shown in Figure 22-5.



```
Currently Selected Profiles
 1*
   User Id No     :  1024 Id: deforres Name:   Lloyd DeForrest
   Project Name   :  Demo Storm                Project Notify      :  NOTIFY        DELETE
   Position       :  BSDIR                     Position Notify     :  Notify        DELETE
   Directorate    :  ECJ1 Directorate          Directorate Notify  :  NOT_NOTIFY    DELETE
   Division       :  Force Integration         Division Notify     :  NOT_NOTIFY
   Branch         :  Admin Branch              Branch Notify       :  NOT_NOTIFY
   Section        :  Ops Briefing/Graphics     Section Notify      :  NOT_NOTIFY
   Cell           :  JSE                       Cell Notify         :  NOT_NOTIFY
 2
   User Id No     :  1024 Id: deforres Name:   Lloyd DeForrest
   Project Name   :  Day to Day Operations     Project Notify      :  NOT_NOTIFY
   Position       :  USER                      Position Notify     :  NOT_NOTIFY
   Directorate    :  ECJ3 Directorate          Directorate Notify  :  NOT_NOTIFY
   Division       :  Division 437              Division Notify     :  NOT_NOTIFY
   Branch         :  Admin Branch              Branch Notify       :  NOT_NOTIFY
   Section        :  Ops Briefing/Graphics     Section Notify      :  NOT_NOTIFY
   Cell           :  JSE                       Cell Notify         :  NOT_NOTIFY
   Userid         :  deforres Lloyd DeForrest  _|       Branch     :                _|
   Project        :                            _|       Section    :                _|
   Directorate    :                            _|       Cell       :                _|
   Division       :                            _|        Position  :                _|
                          |                                 |
                          | | Update Profile Filter |   | Clear Profile Filter | |
                          |                                 |
                               PROJECT: Not Applicable
```

Figure 22-5. Profile Manager Main Window

22.3.1.2 Profile Manager Termination. To exit the Profile Manager computer program:

A. Click on **File > Exit** on the "Profile Manager" menu bar. You will be prompted to confirm the exit request.

B. Click on **OK**. All Profile Manager-related windows vanish.

22.3.2 Profile Manager Menus. The Profile Manager has five menus: File, Edit, Options, Modify, and Help. Choices available in these menus are illustrated in Figure 22-6.

The Profile Manager main window (Figure 22-5) contains two distinct areas: the top portion of the window is where selected profiles are displayed, the bottom is used as a filter.

Also included in this display are the organization "Notify" and "Delete Rights" indicators. When the Notify indicator displays "NOTIFY" next to an organization, the user will be notified when messages are received for that organization. The Delete Rights indicator displays "DELETE," to indicate the user has been given Delete Rights to elements in that organization's folder.

22.3.3 System Profile Maintenance Tasks. The following paragraphs provide the necessary step-by-step actions required to utilize the capabilities provided by the Profile Manager computer program.

22.3.3.1 Viewing Users and Profiles. Upon successful program initialization the Profile Manager main window is displayed.

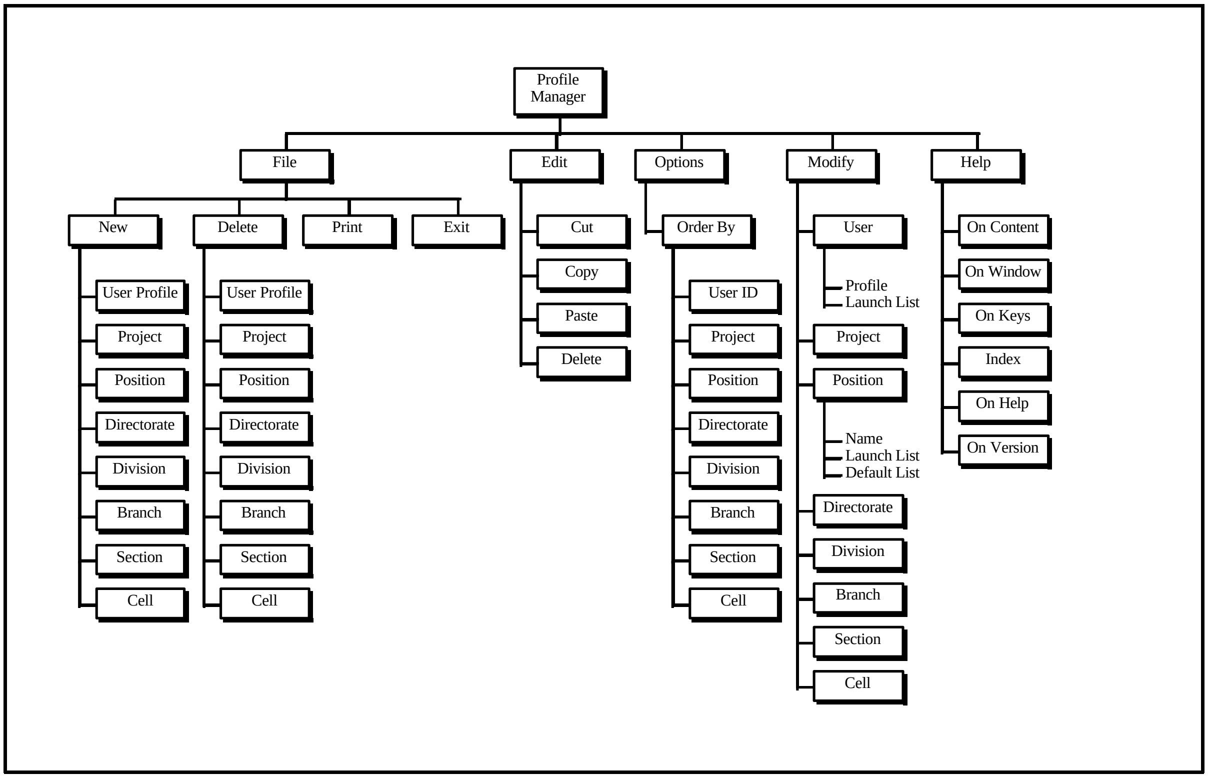


Figure 22-6. Profile Manager Menu Structure

The user profiles displayed in the main window can be filtered according to criteria listed in the bottom of the main window. Each of the filter criteria is selected from a pop-up selection list. For example: selecting user ID alone will show all profiles for a particular user, while selecting any other profile attributes without the user ID will show all users with the chosen profile attributes. To display profile(s) that correspond to a certain filter criterion:

A. Click on a pop-up selection button for profile attributes to be used for the profiles to be listed. The pop-up selection dialog for the selected profile attribute is displayed.

1. Click on the name of the selection to be used for this profile attribute.

2. Click on **Ok/Apply**. The selected name appears in the corresponding profile attribute text field in the main window. Click on **Undo** in the pop-up selection dialog if a selection is to be changed. The last selection will be removed from the main window. Note that the "Update Profile Filter" and "Clear Profile Filter" buttons in the bottom of the main window become active after the first filter profile attribute is entered (these buttons are initially stippled).

B. Repeat step a above for each profile attribute desired.

C. Click on **Update Profile Filter** button on the main window. All user profiles that meet the filter criteria are displayed in the main window with the default profile being marked by an asterisk (*).

D. Click on **Clear Profile Filter** to erase all filter criteria previously selected, and the profiles displayed in the main window. This action results in the "Update Profile Filter" and the "Clear Profile Filter" buttons becoming stippled again.

22.3.3.2 Profile Attribute Maintenance. The attributes that make up the components of a profile are Project, Position, Directorate, Divisions, Branch, Section, and Cell. Some attributes are optional; however, if they are used in a profile, they must have been previously created. While each attribute is created/deleted/modified separately, relationships also exist between some of the attributes that require cross-checking when an attribute is worked on, specifically between Project and Positions, and Project and Cell. The following list describes all attributes:

- **Project.** A project represents one of the GCCS activities that have been defined for a particular facility or facilities in which GCCS is operating. This attribute must be specified when creating a user profile.
- **Position.** This attribute represents a specific task or assignment undertaken by a user. Positions belong to one or more projects; therefore a project name must be selected during the creation of a position.
- **Directorate.** This is an optional attribute.
- **Division.** This is an optional attribute.
- **Branch.** This is an optional attribute.
- **Section.** This is an optional attribute.
- **Cell.** All cells belong to a project, therefore a project name must be selected during creation of a cell. "Cell" is an optional attribute.

A. **Creating a new project.** To create a new project:

1. Click on **File > New > Project** on the Profile Manager menu bar. The "Add New Project" dialog is displayed.

2. Type in the name of the new project (maximum of 25 characters; no special characters are allowed). If the "Default Positions" list is to be used with this new project, click on the **Use Default Positions** button in the "Add New Project" dialog.

3. Click on **Ok/Apply** to save the new project name.

> **NOTE:** For every project created, there must be an associated position. Validation of the project/position pair must be manually performed off-line prior to insertion into a user profile.

B. **Creating a New Position.** To create a new position:

1. Click on **File > New > Position** on the Profile Manager menu bar. The "Add a New Position" dialog is displayed.

2. Since all positions belong to a project, select a project name via the pop-up selection button.

3. Type in the name of the new position (maximum of 8 characters; no special characters are allowed).

4. Type in a description of the position name (maximum of 25 characters).

5. Click on **Ok/Apply** to save the new position name.

> **NOTE:** For every project created, there must be an associated position. Validation of the Project/Position pair must be manually performed off-line prior to insertion into a user profile.

C. **Creating a New Directorate.** To create a new directorate:

1. Click on **File > New > Directorate** on the Profile Manager menu bar. The "Add a New Directorate" dialog is displayed.

2. Type in the name of the new directorate (maximum of 25 characters).

3. Click on **Ok/Apply** to save the new directorate name.

D. **Creating a New Division.** To create a new division:

1. Click on **File > New > Division** on the Profile Manager menu bar. The "Add a New Division" dialog is displayed.

2. Type in the name of the new division (maximum of 25 characters).

3. Click on **Ok/Apply** to save the new division name.

E. **Creating a New Branch.** To create a new branch:

1. Click on **File > New > Branch** on the Profile Manager menu bar. The "Add a New Branch" dialog is displayed.

2. Type in the name of the new branch (maximum of 25 characters).

3. Click on **Ok/Apply** to save the new branch name.

F. **Creating a New Section.** To create a new section:

1. Click on **File > New > Section** on the Profile Manager menu bar. The "Add a New Section" dialog is displayed.

2. Type in the name of the new section (maximum of 25 characters).

3. Click on **Ok/Apply** to save the new section name.

G. **Creating a New Cell.** To create a new cell:

1. Click on **File > New > Cell** on the Profile Manager menu bar. The "Add New Cell" dialog is displayed.

2. Since all cells belong to a project, select a project name via the pop-up selection button.

3. Type in the name of the new cell (maximum of 25 characters).

4. Click on **Ok/Apply** to save the new cell name.

H. **Deleting a Project.** To delete a project:

1. Click on **File > Delete > Project** on the Profile Manager menu bar. The "Delete an Existing Project" dialog is displayed. Note the warning that all profiles assigned to this project will be deleted.

2. Select the project to be deleted via the pop-up selection button.

3. Click on **Ok/Apply** to delete the selected project name.

I. **Deleting a Position.** To delete a position:

1. Click on **File > Delete > Position** on the Profile Manager menu bar. The "Delete an Existing Position" dialog is displayed.

2. Select a project name via the pop-up selection button.

3. Select a position name via the pop-up selection button.

4. Click on **Ok/Apply** to delete the selected position name.

J. **Deleting a Directorate.** To delete a directorate:

1. Click on **File > Delete > Directorate** on the Profile Manager menu bar. The "Delete an Existing Directorate" dialog is displayed. Note the warning that all profiles assigned to this directorate will be deleted.

2. Select a directorate name via the pop-up selection button.

3. Click on **Ok/Apply** to delete the selected directorate name.

K. **Deleting a Division.** To delete a division:

1. Click on **File > Delete > Division** on the Profile Manager menu bar. The "Delete an Existing Division" dialog is displayed. Note the warning that all profiles assigned to this division will be deleted.

2. Select a division name via the pop-up selection button.

L. **Deleting a Branch.** To delete a branch:

1. Click on **File > Delete > Branch** on the Profile Manager menu bar. The "Delete an Existing Branch" dialog is displayed. Note the warning that all profiles assigned to this branch will be deleted.

2. Select a branch name via the pop-up selection button.

3. Click on **Ok/Apply** to delete the selected Branch name.

M. **Deleting a Section.** To delete a section:

1. Click on **File > Delete > Section** on the Profile Manager menu bar. The "Delete an Existing Section" dialog is displayed. Note the warning that profiles assigned to this section will be deleted.

2. Select a section name via the pop-up selection button.

3. Click on **Ok/Apply** to delete the selected section name.

N. **Deleting a Cell.** To delete a cell:

1. Click on **File > Delete > Cell** on the Profile Manager menu bar. The "Delete an Existing Cell" dialog is displayed.

2. Select a project name via the pop-up selection button.

3. Select a cell name via the pop-up selection button.

4. Click on **Ok/Apply** to delete the selected cell name.

O. **Modifying a Project.** To modify a project:

1. Click on **Modify > Project** on the Profile Manager menu bar. The "Modify Existing Project" dialog is displayed.

2. Select the project name to be modified via the pop-up selection button.

3. Type in the new project name (maximum of 25 characters; no special characters are allowed).

4. Click on **Ok/Apply** to modify the selected project name.

P. **Modifying a Position.** Position modification entails the following: modifying the name of a position within a project, modifying the list of launch buttons assigned to a position, and modifying the default list of positions assigned to a new project.

1. To modify a position name within a project:

a. Click on **Modify > Position > Name** on the Profile Manager menu bar. The "Modify an Existing Position" dialog is displayed.

b. Select the project name via the pop-up selection button.

c. Select the old position name via the pop-up selection button.

d. Type in the new position name (maximum 8 characters; no special characters are allowed).

e. Click on **Ok/Apply** to modify the selected old position name.

2. To modify a position launch button list:

a. Click on **Modify > Position > Launch List** on the Profile Manager menu bar. The "Edit Position Launch List" dialog is displayed.

b. Select the position name via the pop-up selection button. A list of all available launch buttons is displayed in the right side of the "Edit Position Launch List" dialog. On the left side are all the launch buttons currently assigned to the selected position. Click on a name in one list to move it to the other.

c. Click on **Ok** to save the assigned launch button list.

3. To modify a position default list:

a. Click on **Modify > Position > Default List** on the Profile Manager menu bar. The "Edit Default Position List" dialog is displayed. The list of commonly used positions is displayed in the right side of the "Edit Default Position List" dialog. On the left side are all the default positions. Click on a name in one list to move it to the other. This default list is not GCCS-related. This data was used for UCOM. Do not use this option until further notice .

b. Click on **Ok/Apply** to modify the default list.

Q. **Modifying a Directorate.** To modify a directorate:

1. Click on **Modify > Directorate** on the Profile Manager menu bar. The "Modify Existing Directorate" dialog is displayed.

2. Select an old directorate name via the pop-up selection button.

3. Type in the new directorate name (maximum of 25 characters)

4. Click on **Ok/Apply** to modify the selected directorate name.

R. **Modifying a Division.** To modify a division:

1. Click on **Modify > Division** on the Profile Manager menu bar. The "Modify Existing Division" dialog is displayed.

2. Select an old division name via the pop-up selection button.

3. Type in the new division name (maximum of 25 characters).

4. Click on **Ok/Apply** to modify the selected division name.

S. **Modifying a Branch.** To modify a branch:

1. Click on **Modify > Branch** on the Profile Manager menu bar. The "Modify Existing Branch" dialog is displayed.

2. Select an old branch name via the pop-up selection button.

3. Type in the new branch name (maximum of 25 characters).

4. Click on **Ok/Apply** to modify the selected branch name.

T. **Modifying a Section.** To modify a section:

1. Click on **Modify > Section** on the Profile Manager menu bar. The "Modify Existing Section" dialog is displayed.

2. Select an old section name via the pop-up selection button.

3. Type in the new section name (maximum of 25 characters).

4. Click on **Ok/Apply** to modify the selected section name.

U. **Modifying a Cell.** To modify a cell:

1. Click on **Modify > Cell** on the Profile Manager menu bar. The "Modify Existing Cell" dialog is displayed.

2. Select a project name via the pop-up selection button.

3. Select an old cell name via the pop-up selection button.

4. Type in the new cell name (maximum of 25 characters).

5. Click on **Ok/Apply** to modify the selected cell name.

22.3.4 User Profile Maintenance. Every entry into this window is done via a pop-up selection dialog and it is here that the Delete Rights can be set for each entry. The mandatory entries are User ID, Project Name, and Position Name.

Additionally, before a position name and/or cell name can be selected, a project name must first be selected.

22.3.4.1 Creating a New User Profile. To create a new user profile:

A. Click on **File > New > User Profile** on the Profile Manager menu bar. The "Add a New User Profile" window is displayed.

1. Click on the pop-up selection dialog buttons for those fields chosen to become part of the user profile.

2. Select the **Grant Delete Rights** button if the user will have the right to delete folders and folder elements contained in the selected organization's folder. The user is granted delete rights if the "Grant Delete Rights" button is pushed in (button shaded).

B. Click on **Ok/Apply**. The entries are then verified, and if valid, the new user profile is added into the system.

22.3.4.2 Delete a User Profile. To delete a user profile:

A. Display the profile to be deleted in the main window, and click anywhere within this profile.

B. Click on **File > Delete > User Profile** on the Profile Manager menu bar. The "Delete User Profile" window containing the selected profile is displayed.

C. Click on **Ok/Apply**. The selected profile is deleted and is not recoverable .

22.3.4.3 Modifying a User Profile. To modify a user profile:

A. Display the profile to be modified in the main window, and click anywhere within this profile.

B. Click on **Modify > User > Profile** on the Profile Manager menu bar. The "Modify an Existing User Profile" window is displayed containing the selected profile for modification. All entries, except User ID, can be modified via pop-up selection buttons.

C. Make all modifications.

D. Click on **Ok/Apply**. The selected profile is modified as per Step c.

22.3.5 Launch List Maintenance. When a profile is assigned to a user by the SA, specific application access or privileges are also assigned. When the users logs on, a window on the GCCS Desktop displays a set of icons that represent the applications available to the user. This is known as a launch window. The SA populates that window by choosing specific applications from the applications in the Available Launch List and inserting them into the user's launch list. The Available Launch List contains all available applications that have been properly installed through the use of the System Installer.

22.3.5.1 Modifying a User Launch List. To modify a user launch list:

A. Click on **Modify > User > Launch List** on the Profile Manager menu bar. The "Edit User Launch List" window is displayed.

B. Select a User ID via the pop-up selection button. All launch buttons available are listed in the right side of the "Edit User Launch List." The left side contains the launch buttons that are assigned to the User ID selected. Click on the right side name to move it to the left side, or click on the left side to move it to the right side.

C. Click on **OK** to save a user launch list.

22.3.6 Profiles Display Order. Once profiles are displayed in the Currently Displayed Profiles area of the main window, the SA has the ability to change the order in which they are displayed. The default ordering is by User ID. Profiles can be ordered (in alphabetical order) according to the following eight criteria: User ID, Project, Position, Directorate, Division, Branch, Section, and Cell.

To order the profiles listed according to a specific criterion:

A. Click on **Options > Order By > <a criterion>**, where <a criterion> is one of the eight criteria listed above. After a short time, the Currently Selected Profiles display in the main window is updated to reflect the order according to the criterion selected. The sort order is as follows: Blanks, Numbers, UPPER CASE LETTERS, and lower case letters.

22.4 System Assign Roles Maintenance

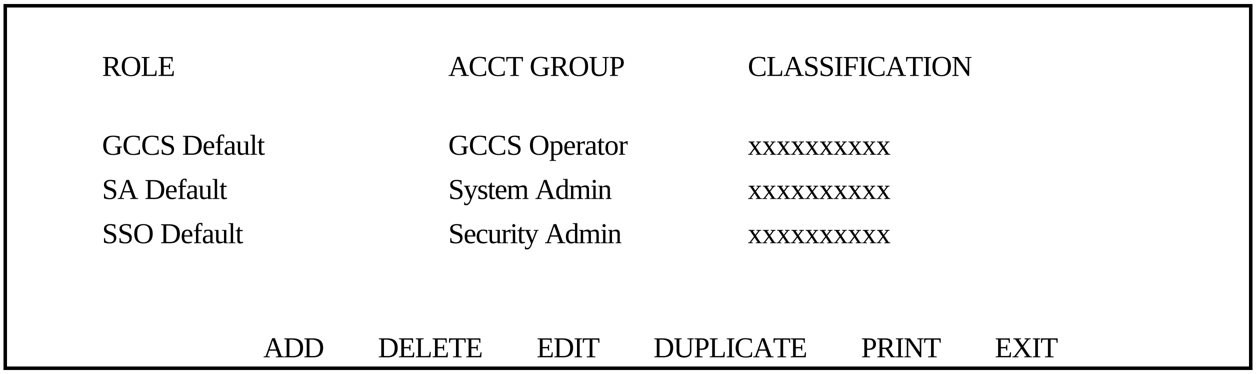
System Assign Roles Maintenance is performed by the SA using the GCCS Desktop Role Manager. The Role Manager is an interactive program that is used to assign roles to users, such as: Security Administrator, System Administrator, and GCCS Operator. This program resides on the GCCS Desktop Dedicated Processor and is started via the Session Manager launch window. The profile performs the following functions:

- Assigns roles to specified account groups by User IDs.
- Deletes roles from specified account groups by User IDs.
- Edits roles to specified account groups by User IDs.
- Duplicates roles of account groups to allow the SA to revise previously entered data to avoid repetitive entry when creating additional roles.
- Print the assigned role of a user.

22.4.1 Role Manager Activation. To activate the Role Manager program, execute the following:

A. Enter **USERNAME: SECMAN** [RETURN]
Enter **PASSWORD** [RETURN]

B. Click twice in rapid succession on the **ROLE** icon on the Session Manager's launch window. Upon successful program initialization the Role Manager main window is displayed, as shown in Figure 22-7.



ROLE	ACCT GROUP	CLASSIFICATION
GCCS Default	GCCS Operator	xxxxxxxxxxx
SA Default	System Admin	xxxxxxxxxxx
SSO Default	Security Admin	xxxxxxxxxxx

Figure 22-7. Role Manager Main Window

22.4.2 Role Manager Termination. To exit the Role Manager, execute the following:

A. Click on **File>Exit** on the Role Manager menu bar. You will be prompted to confirm the exit request.

B. Click on **Ok**. All Role Manager-related windows vanish.

22.4.3 Role Manager Menus. The Role Manager allows the user to add roles to applicable account groups. The structure is shown in Figure 22-8.

22.4.4 Adding a Role to Account Group: Security Admin

A. Click on **Add** in the Role Manager main window (Figure 22-7). The Add Role main menu will appear (see Figure 22-9).

B. Enter name.

C. Enter security.

D. Select **Security Admin** Account Group and click on **OK**.

E. The Security Admin Role Header window will be displayed (see Figure 22-10).

F. To grant permissions to the role, click on the desired permissions in the Permission list in the Security Admin Role Header window, and click **Add**.

Each permission will have a separate screen to enter applicable data.

G. Click on **Edit** only if any one of the permissions needs to be modified.

H. Click on **Menu Access** only if the Security Administrator needs to access the menu for Accounts or Security. Refer to Figure 22-8 to view the structure.

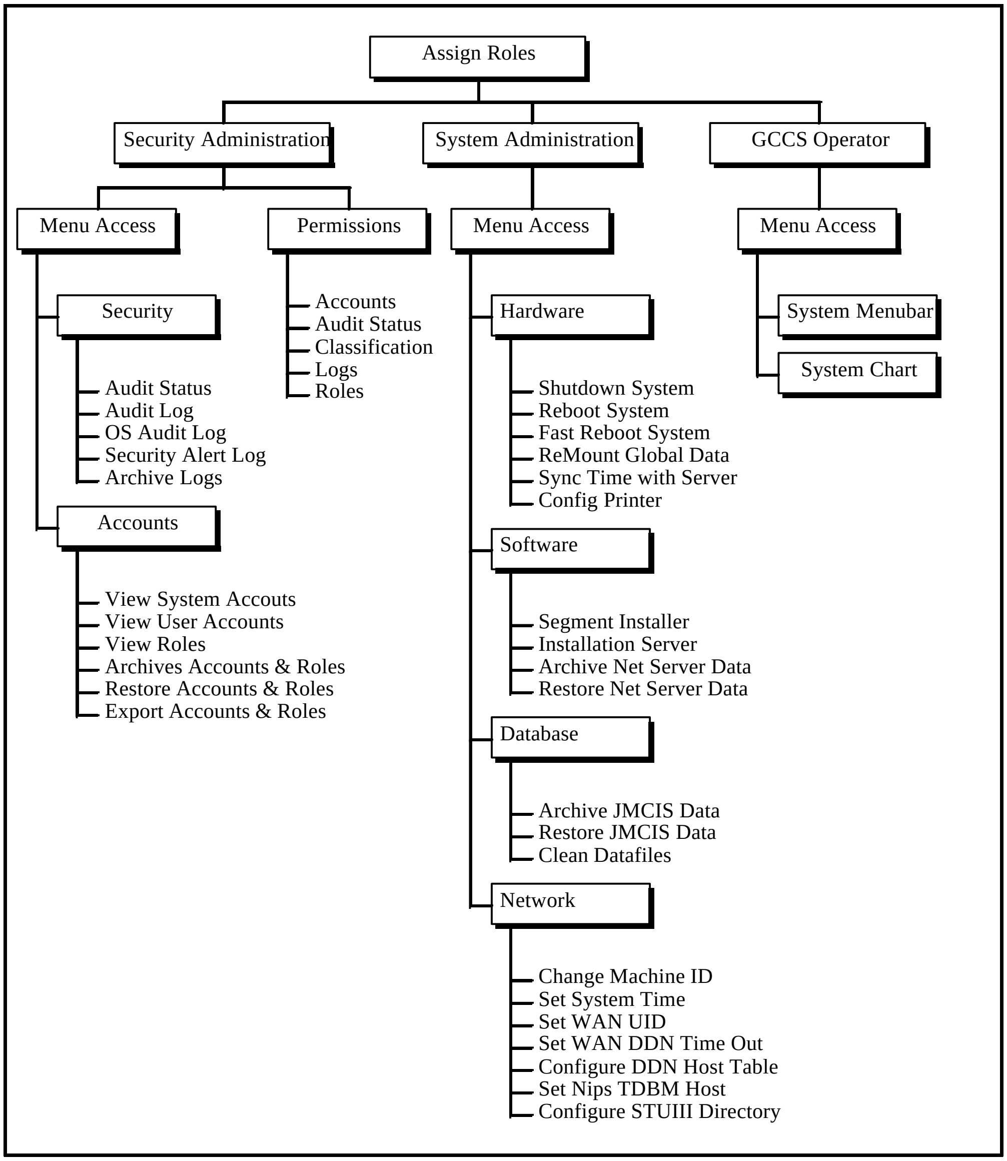


Figure 22-8. Role Manager Menu Structure (Part 1 of 3)

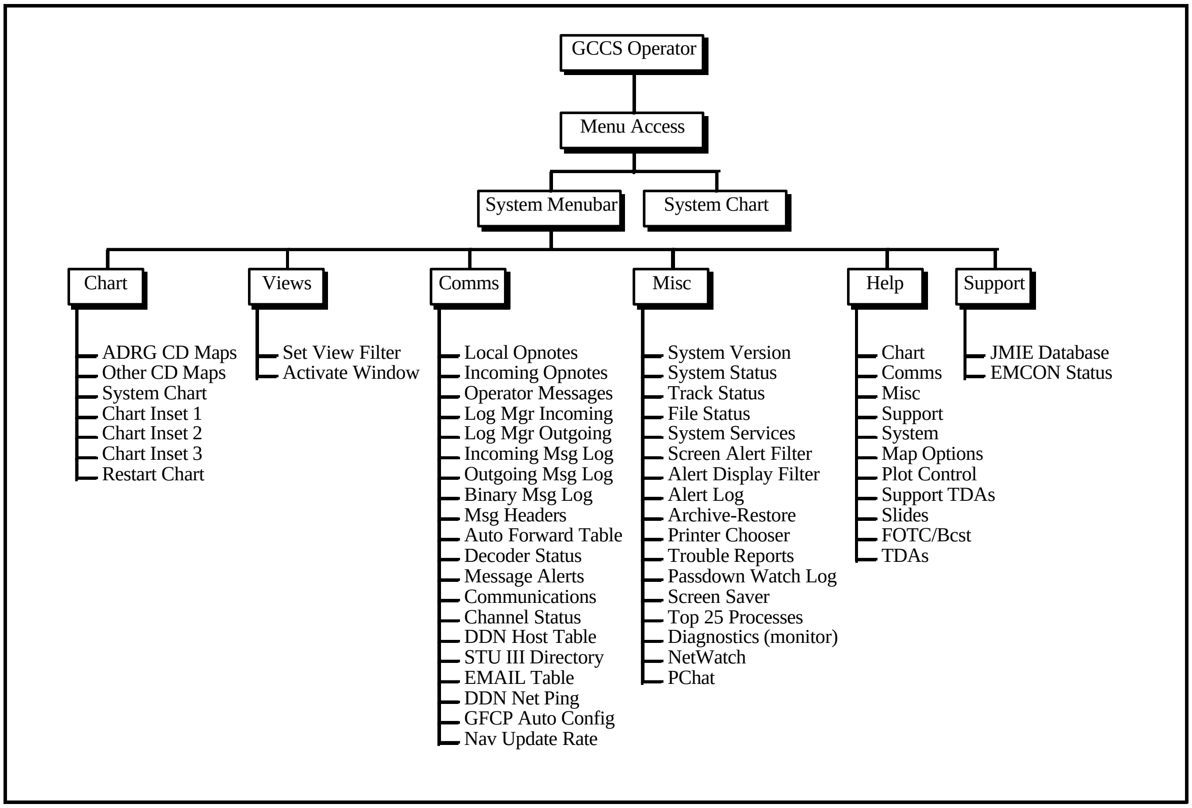


Figure 22-8. Role Manager Menu Structure (Part 2 of 3)

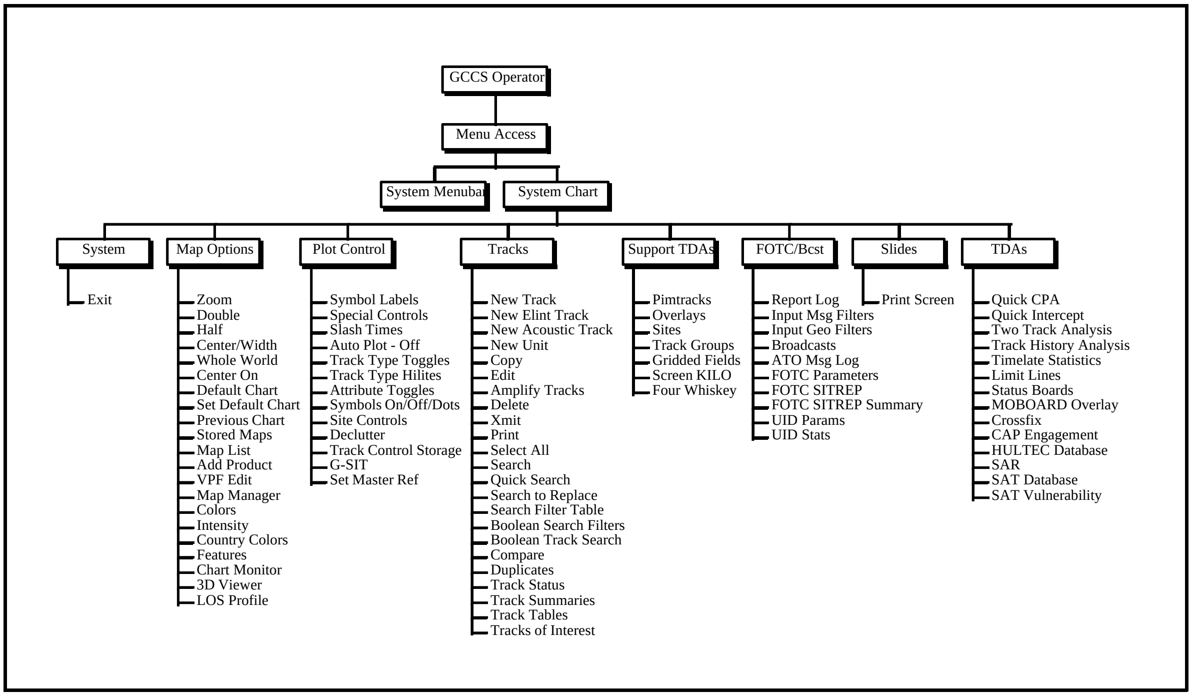
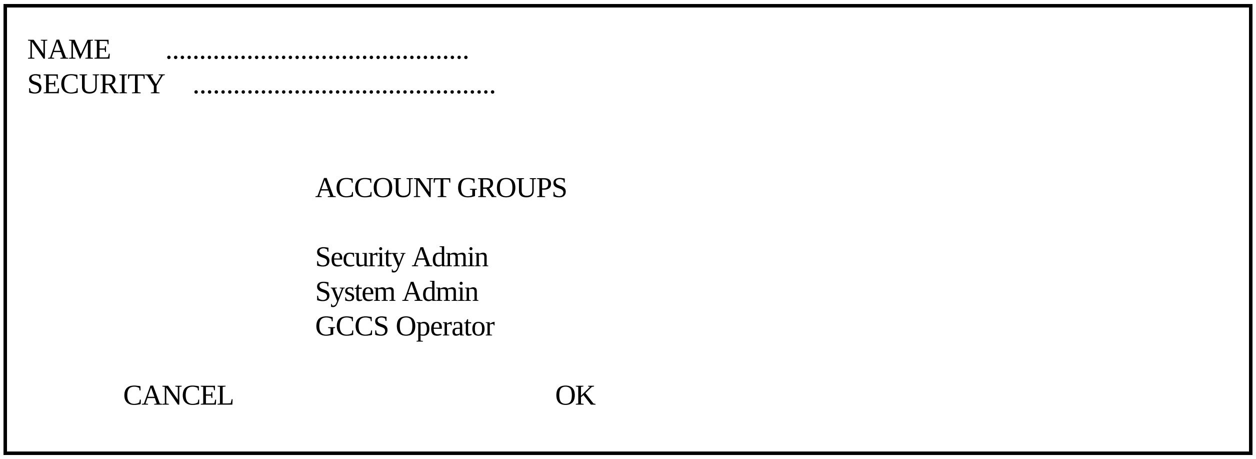


Figure 22-8. Role Manager Menu Structure (Part 3 of 3)

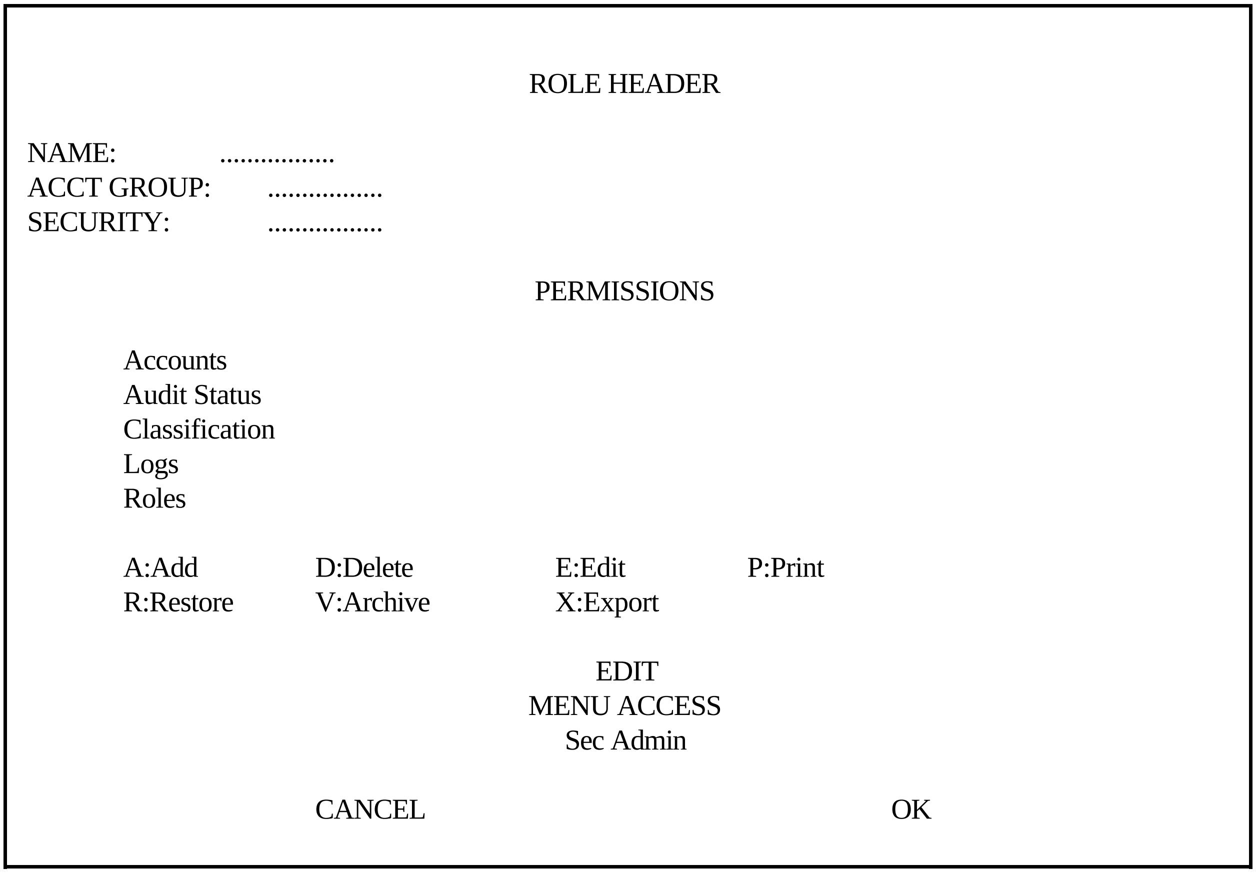

NAME ....
SECURITY ....

ACCOUNT GROUPS

Security Admin
System Admin
GCCS Operator

CANCEL OK

Figure 22-9. Add Role Main Menu



ROLE HEADER

NAME: ....
ACCT GROUP: ....
SECURITY: ....

PERMISSIONS

Accounts
Audit Status
Classification
Logs
Roles

A:Add	D:Delete	E:Edit	P:Print
R:Restore	V:Archive	X:Export	

EDIT
MENU ACCESS
Sec Admin

CANCEL OK

Figure 22-10. Security Admin Role Header

22.4.5 Adding a Role to Account Group: System Admin

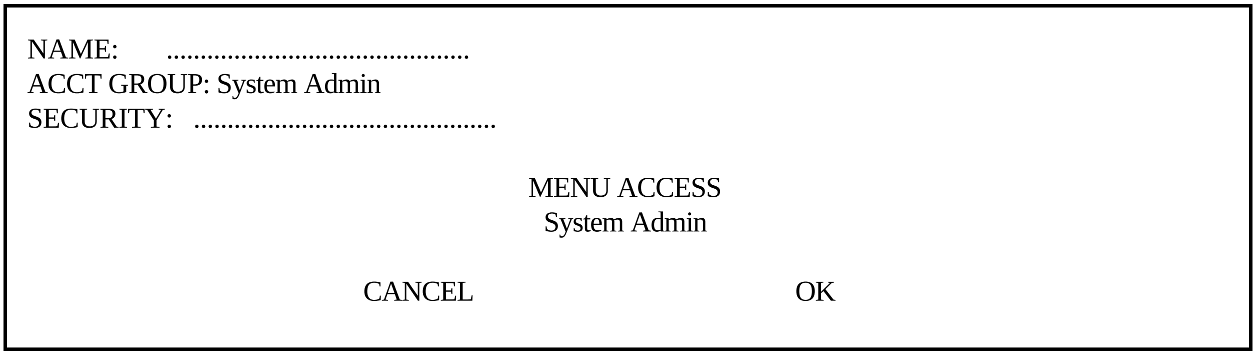
A. Return to the Add Role main menu (Figure 22-9). Select **System Admin** Account Group and click on **OK**. This will bring up the System Admin Account Group window (see Figure 22-11).

B. Enter name.

C. Enter account group.

D. Enter security.

E. Click on **Menu Access** only if the System Administrator needs to access the menu for Hardware, Software, Database, or Network options. Refer to Figure 22-8 to view the structure.



NAME: ....
ACCT GROUP: System Admin
SECURITY: ....

MENU ACCESS
System Admin

Figure 22-11. System Admin Account Group

22.4.6 Adding a Role to Account Group: GCCS Operator

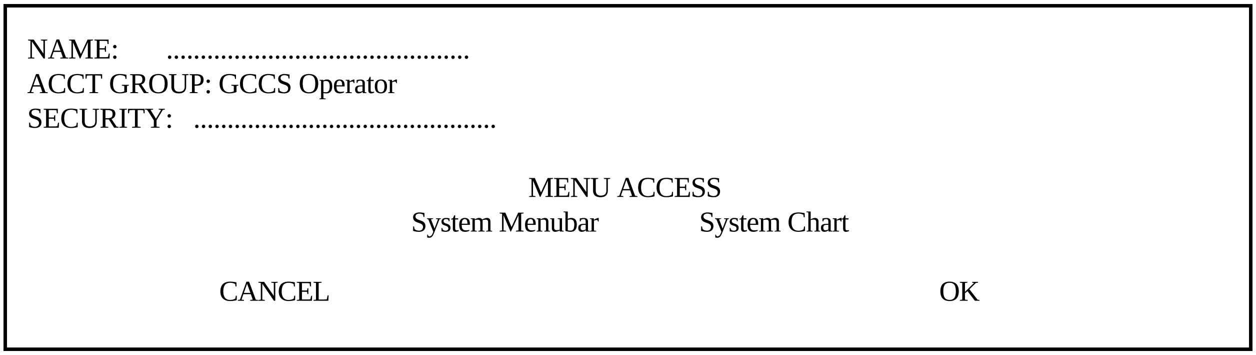
A. Return to the Add Role main menu (Figure 22-9). Select **GCCS Operator** Account Group and click on **OK** (see Figure 22-12).

B. Enter name.

C. Enter account group.

D. Enter security.

E. Click on **Menu Access** only if the SA needs to access the System Menu Bar Options or System Chart Options. Refer to Figure 22-8 to view the structure.



NAME: ....
ACCT GROUP: GCCS Operator
SECURITY: ....

MENU ACCESS
System Menubar   System Chart

Figure 22-12. GCCS Operator Account Group

22.4.7 Deleting a Role from an Account Group

A. In the Role Manager main window (Figure 22-7), click on **Delete** to allow the SA to delete an existing user. A confirmation window will be given.

22.4.8 Edit an Existing Role for an Account Group

A. In the Role Manager main window (Figure 22-7), click on **Edit** to allow the SA to modify an existing user.

22.4.9 Duplicate a Role from an Existing User

A. In the Role Manager main window (Figure 22-7), click on **Duplicate** to allow the user to duplicate SA information in order to create another new user.

22.4.10 Print a Role of a User(s)

A. In the Role Manager main window (Figure 22-7), click on **Print** to invoke the JMCIS printer.

22.4.11 Exit the Role Manager Main Menu

A. In the Role manager main window (Figure 22-7), click on **Exit** to return to the Desktop.

22.5 The Monitor Program

The Monitor launch button runs the Monitor program. This program, under the Options menu (Figure 22.13) presents several useful displays for monitoring the various logs, alarms, and reports.

22.6 The Control Manager Program

The Control Manager launch button contains the **Startup**, **Shutdown**, and other options for selectable hosts. Figure 22-14 presents the menus for the Control Manager. Under the Control menu are the various options. Selection of the **Startup** and **Shutdown** options brings up a window where in the server and host to be started or shut down are selected. Clicking on the **Apply** button executes the command for the selected machines.

I.Selecting the **Kill** and **Initialize** options brings up a window with the list of servers. Highlighting the server and clicking the **Apply** button will execute the selected command for that server.

Selecting the **Execute** option presents a list of hosts and a command input window.

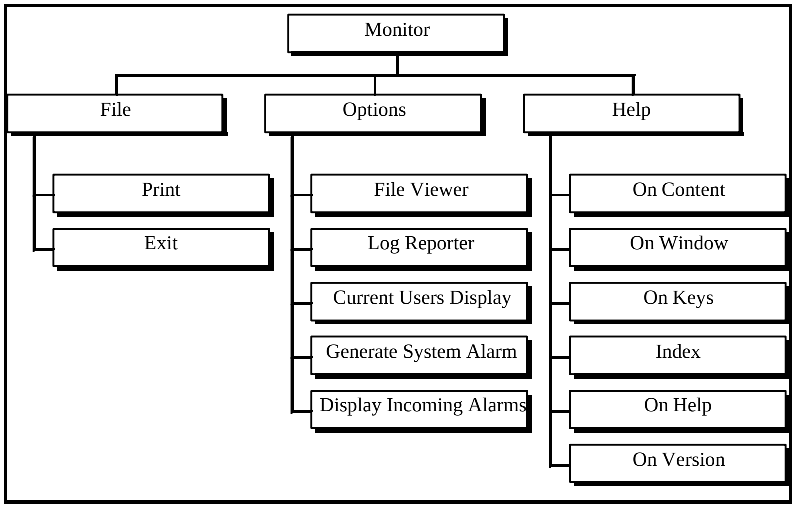


Figure 22-13. Monitor Menu

Selecting the **Report** option currently presents five command options and the host list. The command options are:

- Audit Log
- DEC Processor Status
- Executable List
- Local Password File
- Mac Spt File.

The Local Password File command will cause the password file from the selected host (not the *\/etc/shadow* file) to open for scrolling perusal.

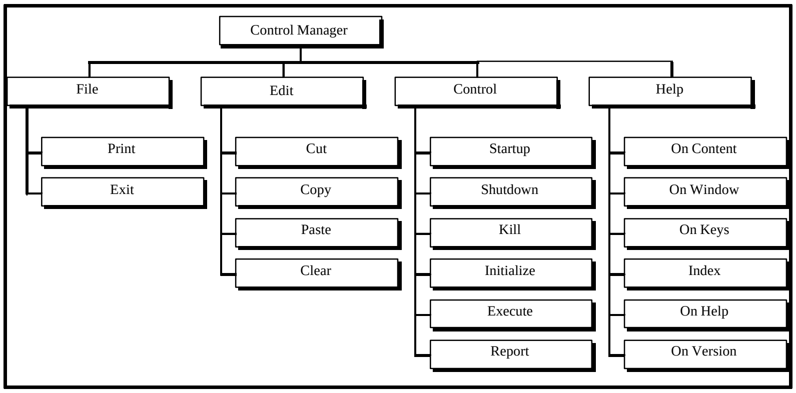


Figure 22-14. Control Manager Menu

APPENDIX C. MSQL DATABASE ADMINISTRATION GUIDE

C.1 Introduction

Mini Structured Query Language (SQL), or mSQL, is a lightweight database engine designed to provide fast access to store data with low memory requirements. As its name implies, mSQL offers a subset of SQL as its query interface. Although it only supports a subset of SQL (no views, subqueries, etc.), everything it supports is in accordance with the American National Standard's Institute (ANSI) SQL specification. The mSQL package includes the database engine, a terminal "monitor" program, a database administration program, a schema viewer, and a C language API. The API and the database engine have been designed to work in a client/server environment over a TCP/IP network.

C.2 Mini SQL Specification

The mSQL language offers a significant subset of the features provided by ANSI SQL. It allows a program or user to store, manipulate, and retrieve data in table structure. It does not support relational capabilities such as table joins, views, or nested queries. Although it does not support all the relational operations defined in the ANSI specification, it does provide the capability of "joins" between multiple tables.

The definitions and examples below depict mSQL key words. (Although they are provided here in upper case, no such restriction is placed on the actual queries).

C.2.1 The Create Clause. The create clause as supported by mSQL can only be used to create a table. It cannot be used to create other definitions such as views. It should also be noted that there can only be one primary key field defined for a table. Defining a field as a key generates an implicit "not null" attribute for the field.

```
CREATE TABLE table_name(
   col_name col_type    [not null|primary key]
   [,col_name col_type     [not null|primary key]]**
)
```

For example:

```
CREATE TABLE emp_details(
   first_name  char(15) not null,
   last_name      char(15) not null,
   dept        char(20)
   emp_id      int primary key,
   salary      int
)
```

The available types are:

```
char(len)
int
real
```

C.2.2 The Drop Clause. The Drop Clause is used to remove a table definition from the database:

```
DROP TABLE table_name
```

For example:

```
DROP TABLE emp_details
```

C.2.3 The Insert Clause. Unlike ANSI SQL, the user cannot nest a Select within an Insert (i.e., the user cannot insert the data returned by a select). Currently, the user must also specify the names of the fields into which the data is to be inserted. The user cannot specify the values without the field name and expect the server to insert the data into the correct fields by default.

```
DELETE FROM table_name
WHERE column OPERATOR value
   [ AND | OR column OPERATOR value]**
OPERATOR can be <, >, =, <=, >=, <>, or like
```

For example:

```
DELETE FROM emp_details WHERE emp_id = 12345
```

The number of values supplied must match the number of columns.

C.2.4 The Select Clause. The Select Clause offered by mSQL lacks some of the features provided by the SQL specification:

- No nested selects
- No implicit functions (e.g., count(), avg()).

It does, however, support:

- Joins
- DISTINCT row selection
- ORDER BY clauses
- Regular expression matching
- Column-to-column comparisons in WHERE clauses.

The formal syntax for mSQL's select is:

```
SELECT [table.]column [,[table.]column]**
FROM table[,table]**
[WHERE [table.]column OPERATOR VALUE
   [AND | OR [table.]column OPERATOR VALUE]**]

[ORDER BY [table.]column[DESC][,[table.]column[DESC]]

OPERATOR can be <, >, =, <=, >=, <>, or like
VALUE can be a literal value or a column name
```

A simple select may be:

```
SELECT first_name, last_name FROM emp_details
WHERE dept='finance'
```

To sort the returned data in ascending order by last_name, and descending order by first_name, the query would look like this:

```
SELECT first_name, last_name FROM emp_details
WHERE dept='finance'
ORDER BY last_name, first_name DESC
```

And to remove any duplicate rows, the DISTINCT operator could be used:

```
SELECT DISTINCT first_name, last_name FROM emp_details
WHERE dept='finance'
ORDER BY last_name, first_name DESC
```

The regular expression syntax supported by LIKE clauses is that of standard SQL:

- '_' matches any single character
- '%' matches) or more characters of any value
- '\' escapes special characters (e.g. '\%' matches % and '\\' matches \ )
- all other characters match themselves.

For example, to search for anyone in Finance whose last name consists of a letter followed by 'ughes', such as Hughes, the query could look like this:

```
SELECT first_name, last_name FROM emp_details
WHERE dept='finance' and last_name like '_ughes'
```

The power of a relational query language becomes apparent when the user starts joining tables together during a select. For example, consider a task where a user has two tables defined, one containing staff details and another listing the projects being worked on by each staff member, and each staff member has been assigned a unique employee number. The user could generate a sorted list of who was working on what project with a query such as this:

```
SELECT emp_details.first_name, emp_details.last_name,
      project_details.project
```

```
FROM emp_details, project_details
WHERE emp_details.emp_id=project_details.emp_id
ORDER BY emp_details.last_name, emp_details.first_name
```

mSQL places no restriction on the number or tables "joined" during a query; therefore if there are 15 tables containing information related to an employee ID in some manner, data from each of those tables could be extracted (albeit slowly), by a single query. One key point to note regarding joins is that the user must qualify all column names with a table name. mSQL does not support the concept of uniquely named columns spanning multiple tables, so the user is forced to qualify every column name if accessing more than one table in a single select.

C.2.5 The Update Clause. The mSQL Update clause cannot use a column name as a value. Only literal values may be used as an update value.

```
UPDATE table_name SET column=value[,column=value]**
WHERE column OPERATOR value
   [AND | OR column OPERATOR value]**

OPERATOR can be <, >, =, <=, >=, <>, or like
```

For example:

```
UPDATE emp_details SET salary=30000 WHERE emp_id=1234
```

C.3 The mSQL Terminal Monitor

Like all database applications, mSQL provides a program that allows a user to interactively submit queries to the database engine. In mSQL, it is a program simply called 'msql'. It requires one command line argument, which is the name of the database to access. Once started, there is no way to swap databases without restarting the program.

The monitor also accepts two command line flags:

- -h *Host* Connect to the mSQL server on *Host.*
- -q Process one query and quit returning an exit code.

The monitor has been modelled after the original Ingres (and the subsequent Postgres) monitor program. Commands are distinguished from queries by backslash prefixes. To obtain help from the monitor prompt, the *\h* command is used. To exit from the program, the *\q* command or an EOF(^D) must be entered.

To send a query to the engine, the query is entered followed by the *\g* command. *\g* tells the monitor to "Go" and send the query to the engine. If the user wishes to edit the last query, *\e* will place the user inside of the vi editor, where the query can be modified. If the user wishes to use an editor other than the vi editor to perform query editing, mSQL will honor the convention of using the contents of the VISUAL environment variable as an alternate editor. When the user has completed the editing, exiting the editor in the usual manner will return the user to mSQL with the edited query placed in the buffer. The query can then be submitted to the server by using the *\g* "Go" command as usual.

The query buffer is maintained between queries not only to enable query editing, but also to allow a query to be submitted multiple times. If *\g* is entered without entering a new query, the last query to be submitted will be resubmitted. The contents of the query buffer can also be displayed by using the *\p* "Print" command of the monitor.

To enable convenient access to database servers running on remote hosts, the mSQL terminal monitor supports the use of an environment variable to indicate the machine running the server (rather than having to specify *-h some.hosts.name* every time the user executes mSQL). Note that this is a function provided by the mSQL terminal monitor, <u>not</u> the mSQL API library, and as such is not available for use with other programs. To use this feature, set the environment variable MSQL_HOST to the name or address of the desired machine.

C.4 mSQL Database Administration

mSQL databases are administered using the *msqladmin* command. Several administrative tasks, such as creating new databases and forcing a server shutdown, are performed using *msqladmin*. Like all mSQL programs, *msqladmin* accepts the '-h *Host*' command line flag to specify the desired machine. The commands available via *msqladmin* are:

- create *DataBase*	Create a new database called *DataBase*
- drop *DataBase*	Delete the entire database called *DataBase*
- shutdown	Tell the server to shut itself down
- reload	Tell the server to reload its access control information
- version	Display various version information from the server.

It should be noted that the server will only accept *create, drop, shutdown,* and *reload* commands if they are sent by the root user (as defined at installation time) and are sent from the machine running the server. An attempt to perform any of these commands from a remote client or as a non-root user will result in a "permission denied" error. The only command a user can execute over the network or as a non-root user is *version*.

C.5 mSQL Schema Viewer

mSQL provides the *relshow* command to display the structure of a database. If executed with no arguments, *relshow* will list the available database. If it is executed with the name of a database, *relshow* will list the tables that have been defined for that database. If given both a database and table name, *relshow* will display the structure of the table including the field names, types, and sizes. Like all mSQL programs, *relshow* honors the *'-h Host'* command line flag to specify a remote machine as the database server.

C.6 mSQL Database Dumper

A program is provided that will dump the contents and structure of a table or entire database in an ASCII form. The program, *msqldump,* produces output that is suitable to be read by mSQL terminal monitor as a script file. Using this tool, the contents of a database can be backed-up or moved to a new database. By virtue of the *'-h Host'* option, the contents of a remote database may be pulled in over the net. This can be used as a mechanism for mirroring the contents of an mSQL database onto multiple machines.

C.7 Access Control

Access control is managed by the *msql.acl* file in the installation directory. This file is split into entries for each database to be controlled. If the file doesn't exist or details for a particular database aren't configured, access reverts to global read/write. This is an example of an acl entry:

```
# Sample access control for mSQL
database=test
read=bambi,paulp
write=root
host=*.Bond.edu.au,student.it.Bond.edu.au
access=local,remote
```

Using this definition, database 'test' can be accessed by both local and remote connections from any host in the *Bond.edu.au* domain except for the *student.it.Bond.edu.au*. Read access is only granted to *bambi* and *paulp*. Nobody else is allowed to perform selects on the database. Write access is only available to *root*.

Control is based on the first match found for a given item. Thus, a line such as "read=-*,bambi" would not get the desired results (i.e., deny access to everyone other than bambi) because -* will also match bambi. In this case, the line would have to be "read=bambi,-*" although the -* is superfluous as that is the default action.

Note that if an entry isn't found for a particular configuration line (such as "read") it defaults to a global denial. For example, if there is no "read" line (i.e., there are no "read" tokens after the data is loaded) nobody will be granted "read" access. This is in contrast to the action taken if the entire database definition is missing, in which case access to everything is granted.

Another feature to note is that a database's entry must be followed by a blank line to signify the end of the entry. There may also be multiple config lines in the one entry (such as "read=bambi,paulp""read=root"). The data will be loaded as though it was concatenated onto the same "read" line (i.e., "read=bambi,paulp,root").

Wild cards can be used in any configuration entry. A wild card by itself will match anything whereas a wild card followed by some text will cause only a partial wild card (e.g., *.Bond.edu.au matches anything that ends in Bond.edu.au). A wild card can also be set for the database name. A good practice is to install an entry with *database=** as the last entry in the file so that if the database being accessed wasn't covered by any of the other rules a default site policy can be enforced.

The acl information can be loaded at runtime using *msqladmin reload*. This will parse the file before it sends the reload command to the engine. Only if the file is parsed cleanly is it reloaded. Like most *msqladmin* commands, it will only be accepted if generated by the root user (or whoever the database was installed as) on the local host.

C.8 Drop_buttons

The *drop_buttons* script located in / *h*/*EM*/*progs* allows the user to list which buttons are stored in the msql gccs database, and to drop buttons if the associated application has been de-installed from all platforms at the site.

The following command will list all buttons stored in the msql gccs database:

```
/h/EM/progs/drop_buttons -l
```

To look for a specific button or group of buttons, enter the following command:

/h/EM/progs/drop_buttons -l {Actual name of button or first few characters}

To drop a button, enter the following:

/h/EM/progs/drop_buttons -l {Actual name of button}

The program will ask for confirmation that the user wishes to drop the specified button.

APPENDIX D. GCCS COE KERNEL DESCRIPTION

D.1 SPARC 1000/2000 (DB Server) With Only SPARCstorage Array(s) (30 x 1.1 GB drives)

This selection creates an ORACLE database server with only SPARCstorage Array(s) attached, not including the internal disk drives contained within the CPU cabinet. A maximum of four SPARCstorage Arrays, each with 30 x 1.1 GB drives, can be configured by the scripts (explained below) provided with this selection. Disk partition maps B.7, B.8, and B.9 should have been used to configure the internal disk drives.

The *load_patches* script loads the SUN-recommended cluster of patches for Solaris 2.3, the NIS+ patches, the Answerbook and NeWSprint patches if applicable, and the other scripts. It also configures the /*etc*/*passwd*, /*etc*/*group*, and /*etc*/*shadow* files for GCCS.

The *vm_install* script installs Volume Manager software needed to configure the SPARCstorage Arrays and the Volume Manager patch. It also creates the / *etc*/*vx*/*disks.exclude* file, which prevents *vxinstall* from initializing non-array disk drives, and sets the path up for root to use the Volume Manager.

The *format_all* script formats all drives that are not defined in / *etc*/*vfstab*. It creates the swap partition on the last drive of the first (if only SPARCstorage Array is available) or the last drive of the second SPARCstorage Array. Finally, it downloads the latest SPARCstorage Array firmware.

The *mk_oracle_group* creates the volumes on the first two SPARCstorage Arrays. If there is only one SPARCstorage Array, all seven volumes / *h*, /*home2*, /*home10*, /*security1*, /*security2*, /*oracle*/*smback*, and /*h*/*USERS* (partition map B.12) will be created on it. The last drive of this array will have been configured as swap space by the *format_all* script. If a second SPARCstorage Array is available the / *security1* and /*security2* volumes and the swap partition will be placed on it. In this instance the last two drives on the first SPARCstorage Array will be used for hot spares. The remaining 28 disk drives on the second SPARCstorage Array will be used to mirror all the volumes on the first, except for the hot spare drives.

The *mk_oracle_group_2* creates two volumes; / *home20* and /*home30* on the third SPARCstorage Array. One drive will be designated a hot spare. The fourth SPARCstorage Array will be configured to mirror the third SPARCstorage Array.

The *kernel_load_remote* or *kernel_load_local* scripts load the second part of the GCCS COE Kernel which contains the *secadm* and *sysadm* account groups and the Executive Manager.

The *gccs_kernel* script completes the setup of the system. This includes preparing the system for networking, DNS, mail, X Windows, and setting the system up as a security auditing server.

D.2 SPARC 1000/2000 "Without" SPARCstorage Arrays

This selection creates an ORACLE database server without SPARCstorage Array(s) attached. This configuration represents the GCCS Database Server with 14 x 2.1 GB hard drives contained in two disk pedestals. The site cannot load the JOPES Core Database (SMDB) on this system. The JOPES Core Database requires a single volume called / *home10* with at least 11 GB of disk space.

The *load_patches* script loads the SUN-recommended cluster of patches for Solaris 2.3, the NIS+ patches, the Answerbook and NeWSprint patches if applicable, and the other scripts. It also configures the /*etc*/*passwd*, /*etc*/*group*, and /*etc*/*shadow* files for GCCS.

The *kernel_load_remote* or *kernel_load_local* scripts load the second part of the GCCS COE Kernel, which contains the *secadm* and *sysadm* account groups and the Executive Manager.

Finally, the *gccs_kernel* script completes the setup of the system. This includes preparing the system for networking, DNS, mail, X Windows, and setting the system up to server as a security auditing server.

D.3 SPARCstation With SPARCstorage Array (18 x 1.1 GB drives)

This selection creates an application or database server with a SPARCstorage array containing 18 x 1.1 GB hard drives and one internal 1.1 GB disk drive. Disk partition maps B.10 should have been used to configure the internal disk drive.

The *load_patches* script loads the SUN-recommended cluster of patches for Solaris 2.3, the NIS+ patches, the Answerbook and NeWSprint patches if applicable, and the other scripts. It also configures the /*etc*/*passwd*, /*etc*/*group*, and /*etc*/*shadow* files for GCCS.

The *vm_install* script installs Volume Manager software needed to configure the SPARCstorage Arrays and the Volume Manager patch. It also creates the /*etc*/*vx*/*disks.exclude* file, which prevents *vxinstall* from initializing non-array disk drives, and sets the path up for root to use the Volume Manager.

The *format_all* script formats all drives that are not defined in /*etc*/*vfstab*. It creates the swap partition and the security auditing partitions (/*sec1* on slice 0 and /*sec2* on slice 7) on the last drive of the SPARCstorage Array. If the system is a Sybase server for the Executive Manager, it creates the four Sybase raw partitions on slices 3 through 6 of the last drive. Finally it downloads the latest SPARCstorage Array firmware.

The *mk_oracle_group* creates three volumes on the SPARCstorage Array; /*h*, /*home1*, and /*home2* (partition map B.14). If the system has been designated as an AMHS server, a fourth volume called /*amhs* will also be created (partition map B.15).

The *kernel_load_remote* or *kernel_load_local* scripts load the second part of the GCCS COE Kernel, which contains the *secadm* and *sysadm* account groups and the Executive Manager.

The *gccs_kernel* script completes the setup of the system. This includes preparing the system for networking, DNS, mail, X Windows, and setting the system up to perform security auditing.

D.4 SPARCstation With SPARCstorage Array (Number of drives not equal to 18)

No script (*mk_oracle_group)* has been written to build volumes on a SPARCstorage Array with an indeterminate number of disk drives. The *load_patches, vm_install, format_all, kernel_load_remote, kernel_load_local,* and the *gccs_kernel* scripts can all be used, but the installer will be required to configure the volumes on the SPARCstorage Array themselves..

D.5 SPARCstation With More Than 2.5 GB of Disk Space (Application Server)

This selection creates or upgrades an application server with a minimum of 2.5 GB of disk space. It is primarily directed toward the standard GCCS application server, which comes with two 1.1 GB and one 2.1 GB hard disk drives. Disk partition maps B.2 or B.3, or variations thereof, should be used for this configuration.

The *load_patches* script loads the SUN-recommended cluster of patches for Solaris 2.3, the NIS+ patches, the Answerbook and NeWSprint patches if applicable, and the other scripts. It configures the / *etc*/*passwd,* /*etc*/*shadow*, and /*etc*/*group* files for GCCS. In the case of an upgrade, several unnecessary accounts are removed from the *passwd*/*shadow* files, the *root .xsession*, *.profile,* and *.cshrc* are modified, permissions are modified on several files, and the / *security1* and /*security2* partitions are created for security auditing.

For a new system the *kernel_load_remote* or *kernel_load_local* scripts load the second part of the GCCS COE Kernel, which contains the *secadm* and *sysadm* account groups and the Executive Manager.

For a system being upgraded, the *kernel_update_remote* or *kernel_update_local* only load the GCCS Version 2.1 *secadm* and *sysadm* account groups. The Executive Manager is upgraded using the *EM_UPGRADE* segment.

The *gccs_kernel* script is only run on new systems, and completes the setup of the system. This includes preparing the system for networking, DNS, mail, X Windows, and setting the system up to perform security auditing.

D.6 SPARCstation With Less Than 1.5 GB of Disk Space

This selection creates or upgrades an application server with less than 1.5 GB of disk space. It is primarily directed toward the low-end GCCS application server, which comes with one 1.1 GB hard disk drive. Disk partition maps B.5, or variations thereof, should be used for this configuration.

The *load_patches* script loads the SUN-recommended cluster of patches for Solaris 2.3 (replacing outdated ones if needed), the NIS+ patches, the Answerbook and NeWSprint patches if applicable, and the other scripts. It configures the / *etc*/*passwd,* /*etc*/*shadow*, and /*etc*/*group* files for GCCS. In the case of an upgrade, several unnecessary accounts are removed from the *passwd*/*shadow* files, the root *.xsession*, *.profile*, and *.cshrc* are modified, permissions are modified on several files, and the / *security1* and */security2* partitions are created for security auditing.

For a new system the *kernel_load_remote* or *kernel_load_local* scripts load the second part of the GCCS COE Kernel, which contains the *secadm* and *sysadm* account groups and the Executive Manager.

For a system being upgraded, the *kernel_update_remote* or *kernel_update_local* only load the GCCS Version 2.1 secadm and sysadm account groups. The Executive Manager is upgraded using the *EM_UPGRADE* segment.

The *gccs_kernel* script is only run on new systems and completes the setup of the system. This includes preparing the system for networking, DNS, mail, X Windows, and serving as a security auditing server.

D.7 SPARCstation With Less Than 600 MB of Disk Space

This selection creates or upgrades an application server with less than 600 MB of disk space. Disk partition maps B.6, or variations thereof, should be used for this configuration.

Several scripts are provided with this selection to build the system. The *load_patches* script loads the Jumbo Kernel Patch (101318), (replacing outdated ones if needed), the NIS+ patches, the Answerbook and NeWSprint patches if applicable, and the other scripts. It configures the /*etc*/*passwd*, /*etc*/*shadow*, and /*etc*/*group* files for GCCS. It also determines if this is an upgrade of a GCCS Version 2.0 system. In the case of an upgrade, the several unnecessary accounts are removed from the *passwd*/*shadow* files, the *root .xsession*, *.profile*, and *.cshrc* are modified, permissions are modified on several files, and the /*security1* and /*security2* partitions are created for security auditing.

For a new system, the *kernel_load_remote* or *kernel_load_local* scripts load the second part of the GCCS COE Kernel, which contains the *secadm* and *sysadm* account groups and the Executive Manager.

For a system being upgraded, the *kernel_update_remote* or *kernel_update_local* only load the GCCS Version 2.1 *secadm* and *sysadm* account groups. The Executive Manager is upgraded using the *EM_UPGRADE* segment.

The *gccs_kernel* script completes the setup of the system in the case of a new system. This includes preparing the system for networking, DNS, mail, X Windows, and creating the /*security1* and /*security2* partitions for security auditing.

D.8 SPARC 1000/2000 With SPARCstorage Arrays and Disk Pedestals

This selection creates an ORACLE database server with both SPARCstorage Array(s) and disk drive pedestals attached. It addresses building systems from the ground up and attaching SPARCstorage Arrays to existing GCCS Version 2.0 systems. A maximum of two SPARCstorage Arrays, each with 30 x 1.1 GB drives, can be configured by the scripts provided with this selection. Disk partition map B.1 should have been used to configure the internal and pedestal disk drives.

The *load_patches* script loads the SUN recommended cluster of patches for Solaris 2.3, the NIS+ patches, the Answerbook and NeWSprint patches if applicable, and the other scripts. It also configures the /*etc*/*passwd*, /*etc*/*group*, and /*etc*/*shadow* files for GCCS. In the case of an upgrade, several unnecessary accounts are removed from the *passwd*/*shadow* files, the *root .xsession*, *.profile*, and *.cshrc* are modified, permissions are modified on several files, and the /*security1* and /*security2* partitions are exported for security auditing.

The *vm_install* script installs Volume Manager software needed to configure the SPARCstorage Arrays and the Volume Manager patch. It also creates the /*etc*/*vx*/*disks.exclude* file, which prevents *vxinstall* from initializing non-array disk drives, and sets the path up for root to use the Volume Manager.

The *format_all* script formats all drives that are not defined in /*etc*/*vfstab*. It also downloads the latest SPARCstorage Array firmware. It also renames the following partitions on the disk drive pedestals: /*h* becomes /*h1* and /*h*/*USERS* becomes /*h1*/*USERS*.

The *mk_oracle_group* creates the two volumes, / *h* and /*home10*, on the first SPARCstorage Array, with the last drive designated as a hot spare. If there is second SPARCstorage Array, it is configured to mirror the first. After the volumes are created and the file systems mounted, the contents of the original / *h*, now /*h1*, is copied to the / *h* on the SPARCstorage Array, and / *h1*/*USERS* is renamed / *h*/*USERS*.

For systems being built from the ground up, the *kernel_load_remote* or *kernel_load_local* scripts load the second part of the GCCS COE Kernel, which contains the *secadm* and *sysadm* account groups and the Executive Manager.

For a system being upgraded, the *kernel_update_remote* or *kernel_update_local* only load the GCCS Version 2.1 *secadm* and *sysadm* account groups. The Executive Manager is upgraded using the *EM_UPGRADE* segment.

The *gccs_kernel* script is only used on new systems and completes the setup of the system. This includes preparing the system for networking, DNS, mail, X Windows, and serving as a security auditing server.